VŠB - Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra telekomunikační techniky

Bezpečné připojování do sítí

Security Access to Networks

2010 **Josef Kratoš**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Josef Kratoš**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Bezpečné připojování do sítí
Security access to networks

Zásady pro vypracování:

Cílem diplomové práce je navrhnout a ověřit bezpečné připojování do síťové infrastruktury malé firmy se dvěma divizemi.
1. Teoretický rozbor problematiky.
2. Návrh bezpečného připojování.
3. Ověření navržené metody.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího diplomové práce.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Pavel Nevlud**

Datum zadání: 20.11.2009

Datum odevzdání: 07.05.2010

prof. RNDr. Vladimír Vašinek, CSc.
vedoucí katedry

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * OSTRAVA *

prof. Ing. Ivo Vondrák, CSc.
děkan fakulty

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Datum odevzdání: 7. května 2010 Podpis:…….....

Poděkování

Rád bych poděkoval vedoucímu diplomové práce, panu Ing. Pavlu Nevludovi, za konzultace, věcné připomínky a vedení při tvorbě této práce. Dále bych chtěl poděkovat rodině a všem přátelům za podporu.

Abstrakt

Cílem diplomové práce je teoretické shrnutí bezpečnostních mechanismů při přístupu do IT infrastruktury se zaměřením na stávající trend mobility pracovníků a jejich potřeby mít přístupná podniková data na služebních cestách i doma vzhledem k vzrůstajícímu významu tzv. práce z domu a dále se zaměřením na podnikové partnery vzhledem k zpřístupnění některých podnikových dat svým zákazníkům. V práci jsou popsány konkrétní systémy spojené se vzdáleným přístupem RAS (Remote Access Service) a také je zde věnována pozornost problematice hesel. Praktická část se zabývá konkrétní konfigurací SSL VPN na zařízení Juniper Network SA6500 a jeho ověření v praxi.

Klíčová slova

RAS, bezpečný přístup, kryptografie, Juniper Network, AAA, VPN, IPsec, SSL VPN, LAN, WLAN, VLAN, firewall, sociální inženýrství, RM OSI model, TCP/IP model, Proxy, TCP/IP, DMZ, heslo, WPA, WEP

Abstract

Diploma work is focused mainly on theoretical describing of security mechanisms for accessing into IT infrastructure considering new trends in mobility of employees and on their need to use company datacenters remotely on business trips or from home offices. Regarding on-line business activities customers or trading partners require access to some company's data and efficient security mechanisms are necessary to be employed. Particular systems associated with security of RAS (Remote Access Service) and login problems are defined as well. Practical part of this work describes configuration of SSL VPN on device Juniper Network SA6500 and its testing in praxis.

Key words

RAS, Security Access, Cryptography, Juniper Network, AAA, VPN, IPSec, SSL VPN, LAN, WLAN, VLAN, Firewall, Social Engineering, RM OSI Model, TCP/IP Model, Proxy, TCP/IP, DMZ, Password, WPA, WEP

Seznam pojmů a zkratek

802.1x	Protokoly pro zabezpečený přístup
AAA	Zkratka pro zařízení sloužicí k autentizaci, autorizaci a účtování
Bot	Automatické servery zapojené do internetu s aplikacemi snažící se prolomit síťové ochrany
DHCP	Server přidělující automaticky IP adresy
DMZ (Demilitating Zone)	Demilitarizovaná zóna
Firewall	Zařízení sloužící k filtrování provozu
Hash	Otisk
IP (Internet Protocol)	Síťový protokol
IPSec (IP Security)	Zabezpečení pro IP síťový protokol
IT (Information Tecnology)	Informační technologie
LAN (Local Area Network)	Lokální síť
MAC Address	Hardwarová adresa – Fyzická adresa
NAT (Network Address Translation)	Překládání IP adres
Port Security	Bezpečnostní nastavení portu na přepínači
RADIUS	Autentizační protokol
RAS (Renote Access Service)	Vzdálený přístup
Realm	Oblast
RM OSI (Reference Model Open System Operation)	Referenční model - ISO standard
Router	Směrovač
RSA šifra	Asymetrická šifra vynalezená autory Rivest, Shamir, Adleman
Sociální inženýrství	Zahrnuje metody a postupy, jak získat důvěru lidí a skrze ně se dostat k důležitým informacím
Subnet	Podsíť – segment sítě oddělený směrovačem od jiné sítě
Switch	Přepínač
TCP (Transport Control Protocol)	Transportní protokol – zabezpečený
Token	Zařízení nebo aplikace generující kód určený k autentizaci
UDP (Uncontrol Delivery Protocol)	Transportní protokol – nezabezpečený

VLAN (Virtual Local Area Network)	Virtuální síť
VPN (Virtual Private Network)	Virtuální privátní síť
WLAN (Wireless Local Area Network)	Bezdrátová síť

Obsah

Součástí diplomové práce je DVD datový nosič.

1 Úvod

Zadání diplomové práce zahrnuje poměrně širokou oblast. Patří zde IP sítě, sítě mobilních operátorů, rádiové spoje, atd. Rozhodl jsem se, že ve své diplomové práci se budu soustředit na IP sítě z důvodu jejich celkového rozšíření ve světě a přemísťování ostatních služeb do IP sítí (viz. klasickou telefonii postupně nahrazuje VoIP).

Pro praktickou část diplomové práce jsem si vybral nasazení VPN SSL v korporaci IT, bude popsáno nastavení SSL VPN na zařízení Juniper SA 6500 a problémy, které se vyskytly po instalaci.

1.1 *Co je bezpečnost v IT*

Úvodem bych přirovnal bezpečnost v celé oblasti IT a vlastně i mimo ní ke sportovnímu klání s tím, že jedna strana se snaží zaskočit protivníka, vyhledává jeho slabé stránky, dává pozor na chyby soupeře a nečekaně útočí. I když slavíme výhru v jednom utkání, další se může vyvíjet zcela obráceně, neočekávaně a s jinou taktikou.

Stoprocentní zajištění je jen ideální stav a riziko napadení roste s hodnotou informace, proto nejvíce zabezpečené jsou finanční a vojenské instituce. Na druhé straně se dají vynaložené prostředky na zabezpečení a jeho úroveň přirovnat k logaritmické funkci, přičemž při stoprocentní bezpečnosti se vynaložené prostředky limitně blíží nekonečnu.

1.2 *Jak se vyvíjel pohled na bezpečnost v IT*

V prvopočátcích, kdy se sálové počítače programovaly přímo ve strojovém kódu z terminálu počítače, stačilo danou místnost s počítačem uzamknout. O prvním zabezpečení počítačů se dá hovořit až s nástupem 70. let 20. století a zavedením multi uživatelských operačních systémů, např. UNIX, který zavedl uživatelské účty zabezpečené jménem a heslem, jenž byla zašifrována symetrickou šifrou DES – dnes již prolomenou [1].

Zabezpečení bylo na začátku přijímáno s nevolí, neboť na akademické půdě se vyznávala svoboda informace a dá se říci, že tato nevole byla příčinou výskytu prvního „hackera“, který prolomil hesla v laboratorním počítači a odeslal je jejich majitelům, aby si zabezpečení zrušili. Ale i přes tuto nevoli systém jmen a hesel přetrval a je hlavním zabezpečením IT systému do dnešní doby. A to hlavně proto, že v té době vývoj IT financovala především armáda. V dalším vývoji došlo i k nezveřejňování zdrojových kódů a vzniku omezujících licencí z důvodu vyšších zisků a utajení firemních postupů před konkurencí [2].

2 Bezpečnostní prostředky

2.1 *Typy útoku*

Nyní se vrátím k bezpečnosti v IT. Na začátku je vhodné specifikovat možné hrozby a na základě těchto hrozeb se mohou aplikovat bezpečnostní opatření. Hrozby se dělí podle různých kriterií. V knize *Kybernetická kriminalita* Jirovský [3] rozděluje hrozby na:

- neúmyslné – vzniklé chybou operátora, nebo programátora,
- úmyslné – zde se útočník - hacker - aktivně snaží proniknout do infrastruktury.

Úmyslné hrozby pak dělí na:

- pasivní – útočník odposlouchává provoz na síti a sbírá pro sebe důležitá data,
- aktivní – útočník ovlivňuje data, která jsou posílána síti.

Další rozdělení hrozeb podle Jirovského je uvedeno v kapitolách 2.1.1 a 2.1.2.

2.1.1 Základní hrozby

Základní hrozby zahrnují hrozby směřující již k zprovozněnému systému. Nepatří zde instalační hrozby.

Základní hrozby se dělí na:

- únik informace – jedná se o prozrazení utajované informace neautorizované osobě,
- narušení integrity – zde je narušena konzistence dat jejich změnou nebo záměnou,

- potlačení služby – útok zabraňuje přístupu k datům oprávněnému subjektu,
- nelegitimní použití – využívání služeb nelegitimní osobou.

2.1.2 Aktivační hrozby

Mezi aktivační hrozby patří hlavně „díry“[1] a škodlivé programy, které je většinou nutné aktivovat, ať už instalováním škodlivého programu, nebo aktivováním určitých částí systému. Aktivační hrozby se dělí na:

- maškaráda – když se jedna identita vydává za druhou a využívá práv legitimní identity,
- obejití řízení – využívá slabiny systému,
- trojský kůň – aplikace provádějí běžnou činnost, ale obsahují škodlivý kód, který umožňuje neoprávněné využití informace třetím subjektem,
- zadní vrátka – jedná se o kód v systémovém programu umožňující obejít bezpečnostní politiky systému.

Uvedl jsem zde pojem „hacker“ a bylo by na místě trochu ho přiblížit. Hacker je člověk, který svými technickými schopnostmi dokáže proniknout do zabezpečených systémů. Jedná se tedy o odborníka. Hackeři bývají často medializováni a spojováni jen s kybernetickými zločiny, ale ne vždy se jedná o zavrženíhodnou činnost. Prvním rozlišovacím kriteriem je důvod, který vede hackera k pokusu o prolomení obrany a zde můžeme využít dělení na základě kloboukové metody[2].

- White hats (bílé klobouky) – jedná se odborníky, kteří často pracují pro bezpečnostní firmy. Ty si je najímají, aby svými útoky prověřili jejich vyvíjené bezpečnostní systémy.

[1] Jedná se o chyby v programu, které útočník zneužívá nestandartními postupy
[2] Dělení parafrázuje hrdiny westernových filmů, kdy kladní hrdinové nosili světlé klobouky a záporní tmavé.

- Black hats (černé klobouky) – jsou opravdu většinou zločinci, kteří nabourávají systémy pro peníze.
- Grey hats (šedé klobouky) – jsou odborníci někde na pomezí obou výše zmíněných.

Z výše uvedeného plyne, že hacker nemusí být spojován jen s kybernetickým zločinem v mnoha případech jde o odborníky nebo studenty informatiky, kteří spíše pomáhají vyvíjet bezpečnostní systémy. Zločinní hackeři se často označují termínem „cracker“. Crackeři často využívají postupy, které byly vyvinuty hackery a využívají je pro vytváření viru a trojských koňů, kteří často napadají systémy s operačním systémem MS Windows.

2.2 *Lidský faktor v bezpečnosti IT – sociální inženýrství*

V předchozí kapitole jsem se věnoval hrozbám a útokům na bezpečnostní IT systémy. Nyní se chci zabývat největší hrozbou, a tou je samotný člověk v systému zabezpečení dat. Průzkumy ukazují, že největší podíl na úspěšnosti útoků zapříčiňuje lidská chyba nebo úmysl poškodit svého zaměstnance, ať již bývalého nebo současného. I nejlepší technické zabezpečení je zbytečné, jestli opakovaně firma neproškolí své zaměstnance, jak se chovat při sdílení dat, jestliže nenastaví velmi pečlivě procesy, které okamžitě upraví přístupová práva při odchodu zaměstnance z firmy, nebo při změně jeho pozice. Důležitá je také loajalita zaměstnanců firmy, nespokojený zaměstnanec představuje pro firmu riziko, že začne pracovat pro konkurenci a předávat ji citlivá data. Samozřejmě musí být spuštěny i kontrolní mechanismy prověřující fungování bezpečnostních procesů a firma musí pružně reagovat na výsledky kontrol.

I když se zdají předcházející mechanismy příliš paranoidní, nesmíme zapomenout, že člověk je velmi důvěřivý a společenský tvor, a tím velmi rychle podléhající útokům sociálního inženýrství. Většina firem se dobře zabezpečí proti útokům zvenčí, ale již často zapomíná, že útok zevnitř je mnohem nebezpečnější, hůře odhalitelný a v mnoha případech mu nelze zabránit.

2.2.1 Zamezení útoku sociálního inženýrství

Jak tedy zamezit útokům pomocí sociálního inženýrství? Je nutné mít informované, vzdělané a loajální zaměstnance. Renomované firmy zabývající se bezpečností doporučují, aby minimálně 50% financí směřujících do bezpečnosti firmy bylo vynaloženo na školení zaměstnanců a vytváření příjemného pracovního prostředí, což má za následek vysoké procento loajálních zaměstnanců.

Útoky sociálního inženýrství můžeme rozdělit do dvou skupin. V jedné je zaměstnanec obětí útoku a v druhé skupině jsou zaměstnanci útočníci.

Pro omezení vzniku zaměstnance útočníka využívajícího sociálního inženýrství je nutné velmi pečlivě vybírat zaměstnance již v době, kdy je ještě uchazečem. Firmy si uvědomují důležitost loajálního zaměstnance, a proto v personálním oddělení je často zaměstnán psycholog, který prověřuje uchazeče – zda zapadne do kolektivu kolegů, jaké jsou jeho hlavní pohnutky pro změnu zaměstnání, atd. V mnoha firmách je u zaměstnance důležitější loajalita než odborná připravenost. Firmy raději vynaloží více peněz na zaškolení, než by podstoupily riziko útoku zevnitř. Jistě nemusím připomínat, že spokojený zaměstnanec stěží poskytne data konkurenci. Firmy, které si uvědomují výhody spokojeného zaměstnance, vynakládají další finanční prostředky na různé společenské akce a další benefity.

Obětí útoku se většinou stávají lide loajální k firmě, kteří podvědomě předpokládají, že i ostatní zaměstnanci jsou loajální, když si nestěžují na poměry na pracovišti. Útočník pak využívá místa, kde se zaměstnanci rádi zastaví na „kus řeči“ s ostatními kolegy a zde získává informace, které ho nakonec dovedou k cíli. Útočník nemusí být zaměstnancem dané firmy, ale přesto má z veřejně dostupných zdrojů dostatek informací pro vytvoření povědomí o firmě, odposlouchá a odpozoruje zvyky, které ve firmě panují a vzbuzuje dojem dlouhodobého zaměstnance nebo obchodního partnera. Útočník se chová tak přirozeně, že nás ani nenapadne ho považovat za vetřelce a slídila. Proto zaměstnanci, kteří jsou potenciální obětí sociálního inženýrství (tedy skoro všichni), by měli být obeznámeni s principy útoku pomocí sociálního inženýrství a

nebezpečím, které hrozí i z poskytnutí zdánlivě nevýznamné informace. Ta může být pro útočníka cenná pro další posun k cíli. Je nutné stanovit pravidla hovoru na otevřenějších místech v podniku, např. v kantýnách, kuchyňkách, kuřárnách, atd. Důležité je vybudování zásad, jak se má zaměstnanec chovat na sociálních sítích. Sociální sítě typu Facebook, Twiter jsou databankou na informace o dané firmě s možností přímo navázat kontakt. I ze sdělovacích prostředků se dovídáme o ochotě lidí sdělovat soukromá data svým virtuálním kamarádům, které znají jen prostřednictvím sociální sítě, což je přivedlo do nesnází. Proto lze předpokládat, že prostředí sociálních sítí se stává dalším velkým nebezpečím pro únik citlivých podnikových informací.

Aby školení o bezpečnosti byla maximálně účinná, když už je nutné na ně vynaložit nemalé finanční prostředky, je vhodné zvolit interaktivní, názornou a zábavnou formu. Jan Ámos Komenský si byl vědom toho, že nejvíce si žák odnese, je-li pro něho učení zábavou – vhodné účastníky aktivně zapojujeme, vytváříme názorné scénky, umístíme vtipné plakáty s daným tématem na vhodných místech, atd.

Zabránit útoku vedeného pomocí sociálního inženýrství se nelze bránit technickými prostředky a kromě bezpečnostního školení zaměstnanců a vytvářením vhodných pracovních podmínek je nutná i distribuce pravomocí a přístupu k důležitým prvkům IT infrastruktury. Jedna osoba by neměla mít přístup ke všem důležitým prvkům. Velmi účinné je dělení infrastruktury do bezpečnostních zón, přičemž ke každé zóně má přístup jiný omezený okruh zaměstnanců. Jestliže se útočníkovi podaří prolomit jednu bezpečnostní zónu, ostatní mu zůstanou uzavřeny a okruh odcizených informaci je mnohem menší [4].

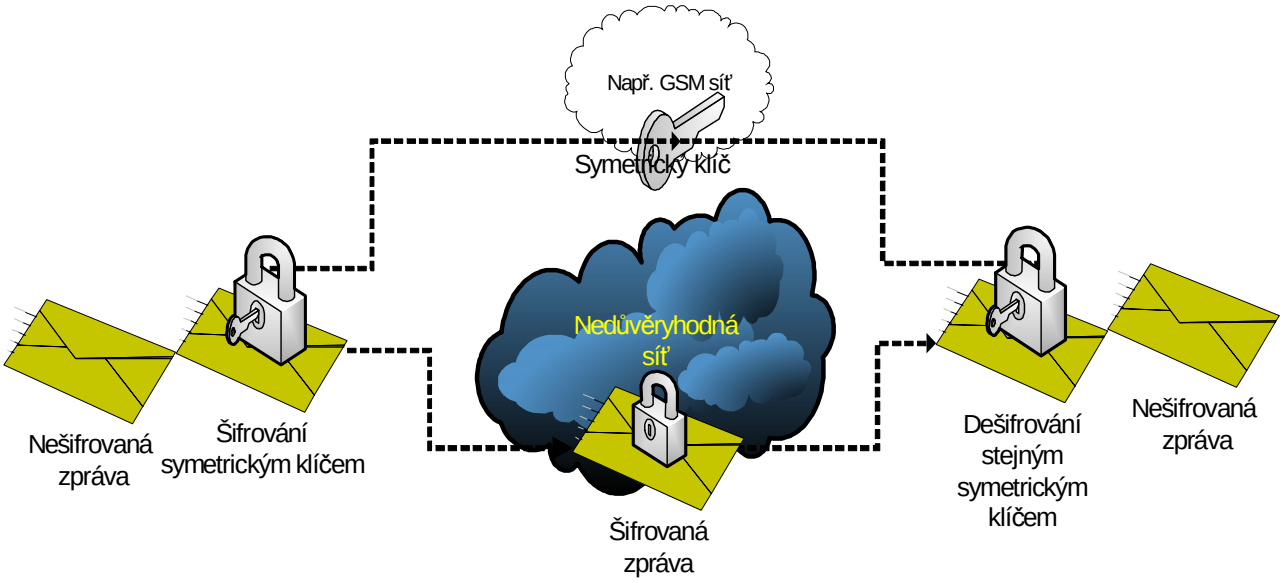
2.3 *Kryptografie*

2.3.1 Šifrování

Doba, kdy šifrování informace se provádělo jen v armádě, již dávno minula. Dnes nikoho nezaskočí, že hovory přes mobilní telefony jsou šifrované, že laptopy, jenž ve

většině případů obsahují citlivá data, mají software, který kryptuje jejich disky. Je už v širším podvědomí, že vzdálený přístup do sítě využívá šifrování provozu mezi stanicí a firemní sítí. Příkladů, kde se využívá šifrovaní v běžném životě okolo nás bychom jistě našli nepřeberné množství. Šifry můžeme rozdělit na symetrické a asymetrické.

- Symetrické šifrování (Obr. 1) – při tomto způsobu šifrování se zpráva kóduje i dekóduje stejným klíčem. Kvalita symetrické šifry závisí na použitém algoritmu a délce šifrovacího řetězce. Symetrické šifry nemají takový nárok na výpočetní výkon jako asymetrické šifrování, proto mohou být použity v malých zařízeních nebo u dat, jež se mají předávat s minimálním zpožděním. Problémem pro symetrické šifrování je předávka klíče. Zde může dojít k odposlouchání klíče, a tím k úspěšnému útoku. Pro předávání symetrického klíče se může využít jiné médium, nebo se symetrický klíč zašifruje asymetrickou šifrou.



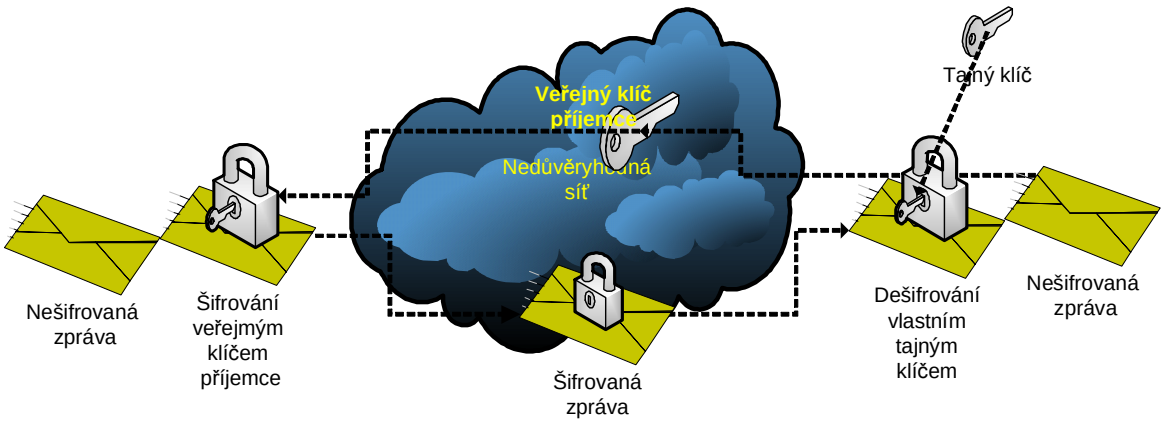
Obr. 1 Symetrické šifrování

Symetrické šifry dělíme na:

- Proudové, při kterých je každý bit samostatně kódován a dekódován. Jejich výhodou je rychlost kódovaní a dekódovaní, proto se využívají hlavně v telekomunikacích. Patří zde např. RC4, FISH a A5.

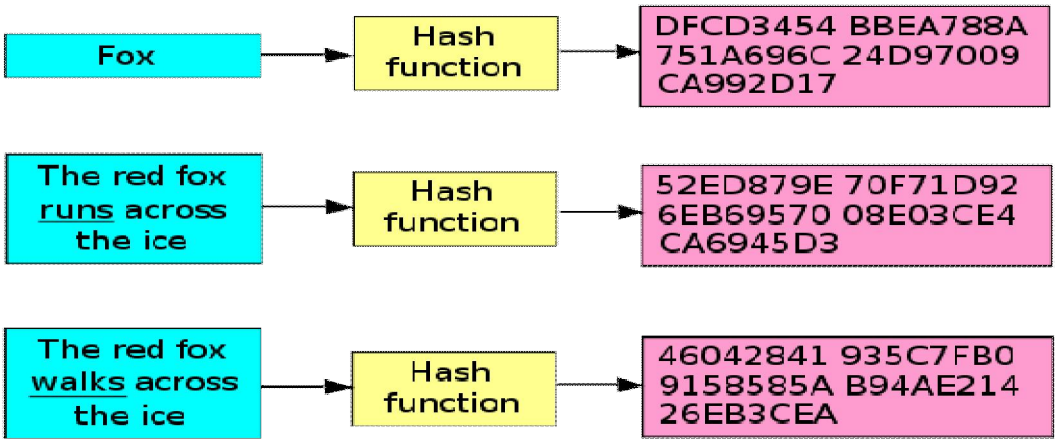
- Blokové, při kterých jsou šifrovány bloky o stejném počtu bitů. Blokové kódovaní je silnější než proudové. Blokové šifry jsou např. AES, DES a RC5.
- Šifrování pro kompresi je například prefixové kódovaní nebo Huffmanova konstrukce. Nevyužívá se pro ochranu přenášených dat [5].

Asymetrické šifrování (Obr. 2) – je založeno na principu vygenerovaní dvou klíčů, které jsou spolu vzájemně matematicky svázány. Základní kriteria pro asymetrické šifrování je nemožnost dekódovaní zprávy stejným klíčem, kterým byla zpráva zakódována a nemožnost odvodit ze znalosti jednoho klíče druhý párový klíč. Zpráva se zašifruje tzv. veřejným klíčem příjemce, který můžeme poslat odesílateli zprávy. Ten zprávu zašifruje tímto klíčem a příjemce obdrženou zprávu dešifruje svým tajným klíčem. Jestliže zprávu odesílatel zašifruje svým tajným klíčem, a pak ji odešleme příjemci, slouží asymetrická šifra jako digitální podpis odesílatele. Příjemce dešifrováním zprávy pomocí odesílatelova veřejného klíče ověří, že zpráva byla odeslána skutečně jim. Nejznámější asymetrická šifra je RSA. Algoritmus využívá Fermatovy věty, která se týká rozkladu prvočísel a Modula. Ještě nebyla objevena metoda jak rozložit velká čísla na prvočísla a není jisté, zda taková metoda vůbec existuje. Pokud by se podařilo takovou metodu objevit, RSA šifra by se stala nepoužitelná [6].



Obr. 2 Asymetrické šifrování

- Certifikát – zde vstupuje do hry certifikační autorita, které věříme, a ta se zaručuje, že jí podepsaný certifikát opravdu náleží danému subjektu. Certifikát lze použít jak k šifrování, tak k ověřování subjektu. Jedná se vlastně také o symetrickou šifru.
- Hashovaní (Obr. 3) – je matematická operace, která i z poměrně velkého množství dat vytvoří krátký řetězec tzv. otisk, který je unikátní a pokud se provede malá změna v datech, ta pak vyvolá poměrně velkou změnu v otisku. Otisk slouží k zajištění integrity dat mezi odesílatelem a příjemcem, který z přijaté zprávy vygeneruje otisk a jeho porovnáním s odesílatelovým otiskem se ověří integrita.



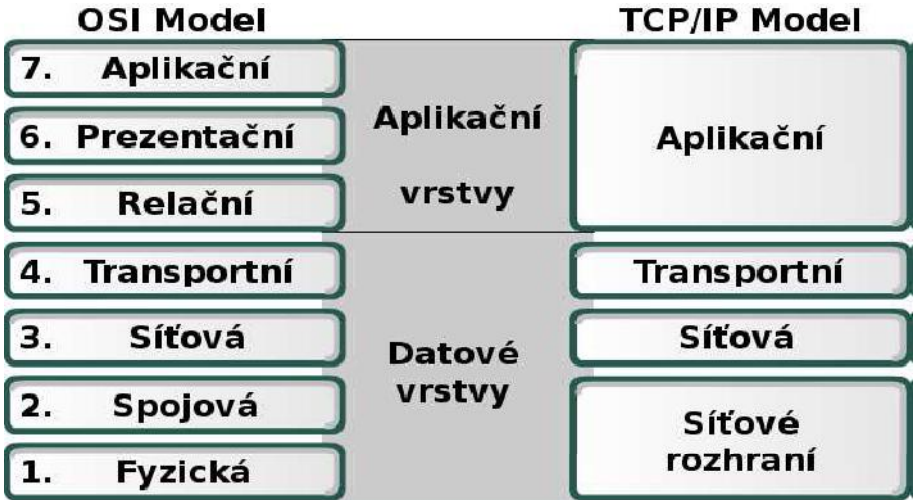
Obr. 3 Hashovaní

3 Bezpečné připojování

Tato kapitola se zabývá bezpečností sítí při útoku z venku – z internetu. Útok pomocí sociálního inženýrství vzrůstá s hodnotou dat ve firemní síti, kdežto útok z venku je prakticky jistý, neboť v internetové síti běží řada automatických botů, které soustavně skenují síť a snaží se najít zranitelný cíl. Z tohoto důvodu a i z důvodů předešlých je nutné mít bezpečné připojení do sítě.

3.1 *OSI model*

Než začnu popisovat zabezpečení sítí, považuji za vhodné zmínit se o principu sítí s využitím RM OSI modelu, který je standardem pro návrh síťových protokolů. OSI model rozděluje síťové procesy do sedmi vrstev, které jsou autonomní a výstup jedné vrstvy je vstupem její sousední vrstvy. Ačkoli je OSI model ISO standardem, pro jeho dlouhé schvalování a jistou složitost byla v praxi dána přednost takzvanému TCP/IP modelu. Oba modely jsou velmi podobné, první a druhá vrstva je spojena u protokolu TCP/IP v jednu a taky pátá až sedmá je spojena opět v jednu vrstvu - aplikační (Obr. 4) [7].



Obr. 4 RM OSI a TCP/IP model

Význam vrstev:

- Aplikační vrstva (protokoly http, SMTP, atd.) – účelem vrstvy je poskytnout aplikacím přístup ke komunikačnímu systému.
- Prezentační vrstva (např. komprese) – má za úkol transformovat data do podoby srozumitelné příjemci.
- Relační vrstva (např. SSL) – řídí výměnu dat, začíná a ukončuje danou relaci. TCP/IP model slučuje tyto vrstvy do jedné a většinou všechny tyto protokoly bývají součástí aplikace, např. webového prohlížeče.
- Transportní vrstva (TCP, UDP) – dochází zde ke fragmentaci dat a jejich zapouzdření, vytváří se segment. Tato vrstva je zodpovědná za navázaní spojení mezi oběma konci komunikace.
- Síťová vrstva (IP, ICMP) – vrstva je hlavně zodpovědná za směrování dat. Vrstva přidává hlavičku s cílovou a zdrojovou adresou k segmentům, a tím vytváří tzv. „paket“.
- Spojová vrstva (Ethernet) – zajišťuje bezpečný přenos dat mezi sousedními zařízeními, paket zapouzdří do rámce, který obsahuje zdrojovou a cílovou adresu zařízení. Je vrstvou, která tvoří rozhraní mezi hardware a software.
- Fyzická vrstva - určuje komunikaci na přenosovém mediu, jedná se o přenos jednotlivých bitů, např. pomocí elektrického signálu, světla, rádiových vln.

3.2 *LAN z pohledu bezpečnosti*

V této kapitole jsou popsána jednotlivá síťová zařízení nebo aplikace (Proxy firevall), jak z pohledu zabezpečení přístupu do sítě, tak i z pohledu monitorování provozu sítě. Musím připomenout, že veškerá zařízení mají i jiné síťové funkce než jen ty, které jsem uvedl v kapitole 3.2.2, ale vzhledem k zaměření této práce nejsou tyto funkce specifikovány blíže.

Musím podotknout, že spravování níže popsaných síťových zařízení vyžaduje z hlediska bezpečnosti přístup pouze zabezpečeným spojením, např. pomocí SSH, nebo ještě lépe vlastním segmentem sítě určeným pouze pro spravování zařízení, kde má přístup pouze autorizovaný personál, tzv. „Management network“.

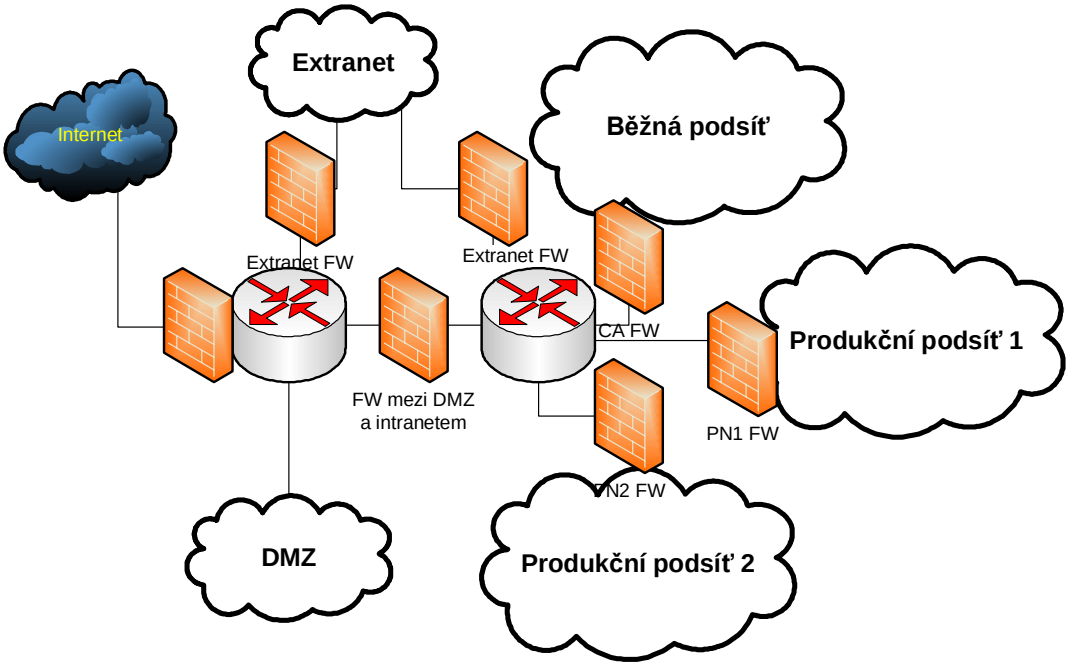
3.2.1 Zóny bezpečnosti v sítích

Bezpečnostní uspořádání sítě se podobá cibuli[3], jak poznamenává Northcutt [8]. Provoz zvenčí je nejprve kontrolován hraničním směrovačem a firewallem, za nimi se obvykle nachází demilitarizovaná zóna (DMZ), obsahující veřejné přístupné služby. V poslední době je u většiny firem povoleno pouze internetové spojení a DMZ se nachází jen v zasedacích a návštěvních místnostech, kde mají přístup i lidé, kteří nejsou zaměstnáni u dané společnosti. DMZ je opět oddělený firewallem a za ním se nacházejí jednotlivé segmenty LAN sítě (Obr. 5):

- běžná podsíť (common area) – síť přístupná všem zaměstnancům firmy,
- produkční podsítě (production area) – prostor, kde jsou spuštěny produkční systémy a je zpřístupněna konkrétním zaměstnancům,
- extranet – síť určena pro zákazníky společnosti,
- popřípadě další subnety.

Jednotlivé elementy jsou samozřejmě opět odděleny firewally a v síti jsou ještě rozděleny další bezpečnostní prvky, např. IPS. Úroveň bezpečnosti u sítí velmi záleží na kvalitním návrhu sítě a až pak na technických bezpečnostních zařízeních [9].

[3] Z vnějšího pohledu se nám jeví celá síť jako souhrn sítí, do kterých se dá postupně pronikat. I na firevallu se většinou definují bezpečnostní oblasti pomocí zónových čísel, např. Cisco ASA FW má zónu 100 jako nejvýše důvěryhodnou a s klesajícím číslem důvěryhodnost sítě klesá.



Obr. 5 Příklad síťové topologie

3.2.2 Síťová zařízení z pohledu bezpečnosti

3.2.2.1 Směrovač

Router neboli směrovač je základním stavebním prvkem v TCP/IP sítích a je hlavně určen k směrování paketů v síti. Směrovače pracují na třetí vrstvě RM OSI modelu. Směrovaní je buď statické, tedy ručně nastavené, nebo dynamické, kdy se směrovač naučí posílat pakety pomocí jednoho ze směrovacích protokolů (RIPv2, OSPF IS-IS, EIGRP, BGP). Směrovače oddělují jednotlivé sítě, zde můžeme umístit paketové filtry a tím ovlivnit směrování jak podle zdrojové adresy, tak i podle cílové adresy, např. je možné nastavit směrování pro příchozí pakety z určité zdrojové adresy na rozhraní Null, a tím zamezit přístup do dalších segmentů sítě pro danou adresu. Směrovače chrání hlavně přístup do sítě z vně sítě. Paketový filtr může být i samostatné zařízení.

Moderní směrovače již mají v sobě integrovány další moduly, a tak mohou vykonávat další síťové funkce jako firewall, DHCP, IDS, VPN brány a DNS.

3.2.2.2 Přepínač

Přepínač neboli switch slouží k přeposílání rámců v jednom segmentu sítě a pracuje na druhé vrstvě RM OSI modelu. Přepínače jsou většinou první zařízení pro transport dat od uživatele. Z pohledu bezpečnosti zde můžeme nastavit „port security“, což nám umožňuje filtrování provozu pomocí hardwarové adresy – MAC adresy, nebo je možné na přepínačích nastavit autentizaci za pomocí autentizačního serveru, pak se musí uživatel přihlásit při zahájení provozu v síti. K tomu slouží protokol 801.1x. Tím se zamezuje útokům ze vnitř sítě.

Moderní přepínače umožňují nastavení VLAN, a tím logické oddělení provozu dat a počítačů pracovníků různých oddělení. Pro komunikaci mezi VLANy jsou nutné směrovače, nebo L3 přepínače[4], což zvyšuje bezpečnost v síti a snižuje náklady na infrastrukturu sítě, neboť VLANy lze nastavit tak, že procházejí několika směrovači, doslova je lze „protáhnout“ celým segmentem sítě.

Přepínače mají rovněž další bezpečnostní funkce jako např. DHCP snooping, který zabraňuje uživateli připojit si svůj vlastní DHCP server, čímž by mohl oklamat koncové stanice.

3.2.2.3 Stavový firewall

Pracuje na čtvrté vrstvě RM OSI modelu a je pokročilejší verzí paketového filtru. Zařízení dokáže rozeznat zda příchozí spojení je reakcí na povolené odchozí, pokud ano, pak provoz propustí, v opačném případě provoz zakáže. Z toho vyplývá, že stavový firewall má plnou kontrolu stavů TCP spojení i UDP streams - proudů.

[4] L3 přepínače v sobě kombinují přepínač a směrovač. Nacházejí se většinou v páteřní síti.

firewall má většinou i NAT/PAT funkci, která původně nebyla určena jako bezpečnostní prvek, ale díky principu překladu adres se stal oblíbeným bezpečnostním prvkem.

3.2.2.4 Proxy firewall

Proxy firewall neboli „proxy server“ pracuje jako prostředník mezi uživatelem a venkovním prostředím, což má za následek, že veškerý provoz vypadá, jako by pocházel od proxy firewallu. Stejně tak i venkovní provoz je vždy směrován na proxy firewall a ne na zařízení ve vnitřní LAN, čímž je vnější síť (např. internet) zcela oddělena od vnitřní sítě. Proxy firewall pracuje na aplikační vrstvě a rozeznává protokoly a typ dat, která přes něj tečou a dokáže tato data filtrovat nebo modifikovat. Proxy firewall dokáže zabránit uživatelům přístup na přesně určené webové stránky, popřípadě znemožní používat definované aplikace.

3.2.2.5 IDS

Intrusion Detection Systems kontrolují provoz v síti a snaží se detekovat nestandardní spojení. IDS neumí detekované spojení zastavit, ale může spolupracovat s firewallem, který provoz zastaví, nebo pouze zasílá informaci administrátorovi sítě. IDS pracuje na principu vyhledávání určitých signatur.

3.2.2.6 IPS

Intrusion Prevention Systems pracují podobně jako IDS, ale již dokáží filtrovat zjištěné hrozby. IPS pracuje na všech vrstvách RM OSI modelu [10].

3.2.2.7 Koncové stanice

Zabezpečení koncových stanic je důležitou součástí bezpečného přístupu do sítě, protože bezpečná síť není jen otázkou bezpečnostních síťových zařízení, ale systémem řetězově spojených, vzájemně sladěných a navzájem se doplňujících prvků.

Z tohoto pohledu je nutné, aby uživatelé měli na svých stanicích nastaveno jen tolik práv, kolik je nezbytné pro vykonávání jejich práce, a tím se zamezí ovlivňování celého

systému. Řada virů a trojských koňů nedokáže úspěšně infikovat počítač, jestliže nemá dostatečná práva k operačnímu systému.

Přístup do každé stanice by měl být chráněn jménem a heslem nejlépe za pomocí autentizačního serveru, např. RADIUSu. Pochopitelně z hlediska bezpečnosti je vhodné mít dostatečně dlouhé heslo obsahující malá a velká písmena, číslice a speciální znaky, viz. Tab. 1 [3]. Problémem je zapamatovatelnost takových hesel. Zde je vhodné využít speciální software pro ukládání hesel jako je například KeePass Password Safe[5]. Tyto aplikace umožňují mít i uložený odkaz na URL adresu, což zase vede k neukládání hesel ve webových prohlížečích, protože uložená hesla ve webových prohlížečích opět představují bezpečnostní hrozbu. Samozřejmostí je automatické vymazaní uložených dat ve schránce po několika desítkách sekund.

heslo	odhad doby na prolomení
4 velká nebo malá písmena	několik sekund
4 velká a malá písmena v různé kombinaci	několik sekund
4 velká a malá písmena a číslice v různé kombinaci	několik sekund
5 velkých nebo malých písmen	minuta
5 velkých a malých písmen v různé kombinaci	6 minut
5 velkých a malých písmen a číslic v různé kombinaci	15 minut
8 velkých nebo malých písmen	58 hodin
8 velkých a malých písmen v různé kombinaci	21 měsíců
8 velkých a malých písmen a číslic v různé kombinaci	7 let
10 velkých nebo malých písmen	5 let
10 velkých a malých písmen v různé kombinaci	4648 let
10 velkých a malých písmen a číslic v různé kombinaci	26984 let

Tab. 1 Odhad času na prolomení hesla [3]

Na problematiku kolem hesel zareagovaly některé firmy vývoje přihlašovacích systémů (např. společnost RSA). Společnost RSA nabízí produkt RSA SecurID založený na

[5] www.keepass.info

použití hardwarových nebo softwarových tokenů (Obr. 6). Tokeny zajišťují dvojfázovou autentizaci – našim přiděleným PINem a kombinací znaků na tokenu měnících se po určitém čase. Pro úspěšné přihlášení musí uživatel skombinovat PIN a tokenové heslo. Tokenové heslo je generováno pomocí asymetrické šifry. Zařízení, ke kterému se chce uživatel přihlásit, odešle přihlašovací informace na autentizačni server, který zná PIN, a na kterém běží algoritmus pro generování shodného tokenového hesla. Autentizační server a koncové zařízení, na které se chceme přihlásit, musí mít synchronizovaný čas. Tato metoda je prakticky neprolomitelná, za dodržení základních bezpečnostních pravidel, jako je držení PINu v tajnosti a odděleně od tokenu.

Obr. 6 HW token; SW token

V poslední době se objevují biometrické metody ověřování uživatele, jako jsou např. daktyloskopické čtečky u laptopů. Tyto biometrické bezpečnostní prvky jsou zatím hodně jednoduché a ještě je čeká určitý vývoj, něž se stanou bezpečným prostředkem pro přihlášení. U těchto biometrických metod existují obavy i z možného odcizení identity při odcizení dat obsahujících biometrická hesla.

3.3 *Vzdálený přístup*

Je trendem dnešní globalizované doby, kdy nadnárodní korporace mají pobočky po celém světě se stává nezbytností nejen bezpečně propojovat jednotlivé sítě pomocí LAN to LAN VPN, ale umožnit vzdálený přístup některým vzdáleným zaměstnancům. V globalizovaném světe firmy mají odběratele i dodavatele z celého světa a jim je opět

nutné bezpečně zpřístupnit některá citlivá data (ne všechna) z korporátní sítě. Dovoluji si tvrdit, že internet (propojené IP sítě) – má pro světový obchod stejný význam jako zavedení papírových peněz, vynález spalovacího motoru nebo vynález telegrafu.

A možná i větší, neboť přiblížil v podstatě jakýkoli kout naší planety pouze na čas, který je potřebný na jedno kliknutí myší. V kapitole se pojednává o VPN technologii, která bezpečně zpřístupňuje domovskou síť z různých koutů světa, což otevírá nové možnosti pro manažery cestující za zákazníky po celém světě, kteří vždy mají aktuální informace z mateřského podniku aniž ho cestou navštívili. Umožňuje jim také ihned reagovat na nenadálé situace v mateřské firmě, aniž by museli přerušit služební cestu nebo situaci řešit opožděně.

Samozřejmě i zákazníci, kterým partnerská firma zpřístupní část svých dat, mohou ihned reagovat na nové nabídky firmy, zúčastňovat se jednání na dálku, což opět snižuje náklady obou stran. Na začátku této stěžejní kapitoly považuji za vhodné zmínit se o autentizaci, autorizaci a účtování, tzv. AAA.

3.3.1 AAA

Authentication, Authorization, Accounting (AAA) je základní nástroj pro bezpečný přístup do IT infrastruktury. Jak je výše zmíněno jedná se o:

- Autentizaci – ověření uživatele. Nejčastěji se provádí za pomocí uživatelského jména a hesla. Pro vyšší bezpečnost je použita vícefaktorová bezpečnost, kdy k heslu se ještě přidá např. RSA token. Poslední, stále se rozvíjející metodou je biometrická autentizace, která v budoucnu zaujme velmi významné místo.
- Autorizace – kontroluje přidělená práva. Úkolem autorizace je tedy rozhodnout, zda uživatel je oprávněn přistoupit k dané službě v daný čas. Probíhá až po autentizaci, kdy už je ověřeno, o koho se jedná.
- Účtování – sledování činnosti uživatele. Umožňuje sledovat využívaní služby ověřeným a autorizovaným uživatelem a výsledků účtování může být využito

například při fakturaci, nebo při vytváření cílené nabídky pro zákazníka. Velmi často využívají internetoví prodejci účtování pro sledování, o které produkty je zájem.

Je pochopitelné, že maximální bezpečné uchovávání AAA údajů je pro uživatele stěžejní [11].

3.3.2 VPN

Virtuální privátní síť (VPN) umožňuje bezpečně propojit přes internet dvě sítě v různých lokacích, které se pak pro uživatele tváří jako jedna transparentní síť. Bez použití VPN technologie by firma musela pronajmout zvláštní linku na propojení dvou poboček a platit za ni, i když zrovna není využívána. VPN technologie pracují mezi 2. a 3.vrstvou, na 3. vrstvě a mezi 4. a 5. vrstvou referenčního modelu OSI.

Typy VPN se dělí podle dvou kritérií, tzv. Peer-to-Peer a Overlay VPN. O spojení mezi koncovými stanicemi (Peer-to-Peer) se zmíním jen okrajově, jsou to např. VPN protokoly.

- L2TP VPN je z pohledu bezpečnosti rychleji prolomitelný protokol a používá se mezi koncovými uživateli, kteří se vzájemně musí autentizovat.
- L2F VPN je Cisco proprietární protokol pracující na 2. vrstvě RM OSI a umožňuje sdílení ISDN, modemové linky, routerů, serverů a dalších zařízení.
- PPTP VPN byl vytvořen firmou Microsoft společně s 3COM a Ascend a umožňuje jednoduchou implementaci mezi zařízeními s Windows platformou.
- MPLS VPN pracuje mezi 2. a 3. vrstvou RM OSI. MPLS má velký význam pro poskytovatele připojení, kdy bezpečně propojí pobočky několika firem na jedné lince tak, že se firmy vzájemně nevidí.

Overlay VPN (překrývající VPN) pracuje na principu překrytí fyzické síťové infrastruktury virtuálním tunelem. Vytvořený VPN tunel umožňuje bezpečné propojení dvou oddělených sítí nebo uživatelského počítače s domovskou sítí. Provoz ve VPN

tunelu je většinou šifrovaný. V následujících podkapitolách jsem popsal její dva hlavní protokoly – IPSec a SSL VPN [12].

3.3.3 IPSec

IPSec VPN je stěžejní metodou vzdáleného přístupu do domácí sítě. IPSec pracuje na 3. vrstvě RM OSI. IPSec, což znamená „IP security“, rozšiřuje IP protokol o bezpečnostní složku založenou na autentizaci a šifrování každého IP paketu. Díky zabezpečení na síťové vrstvě umožňuje transparentní neodposlouchatelný přenos jakémukoli provozu, na rozdíl od zabezpečení na vyšších vrstvách RM OSI, která vyžadují podporu od aplikací provádějících výměnu dat .

IPSec má několik stěžejních součástí, jedná se tedy o soubor protokolů.

- ISAKMP (Internet Security Association and Key Management Protocol) vyjednává a řídí bezpečné spojení mezi koncovými klienty.
- IKE protokol (Internet Key Exchange Protocol) je zodpovědný za bezpečnou výměnu synchronních klíčů přes nebezpečnou síť – internet. Pro bezpečnou výměnu těchto klíčů používá privátních a veřejných klíčů. Využívá k tomu Diffie-Hellman (D-H) skupin (algoritmus asymetrické kryptografie). Algoritmus D-H není odolný vůči útoku Man-in-the-Middle tedy „záškodník uprostřed“, proto je nejprve nutné zajistit autentizační mechanizmus např. pomocí „pre-shared key“, což je heslo přednastavené na obou stranách spojení. IKE je zodpovědný za vyjednání charakteristiky SA (Security Association), což je zabezpečený kanál mezi koncovými body spojení. Dále je zodpovědný za automatické generování a obnovu klíčů.

  IKE pracuje v následujících fázích:

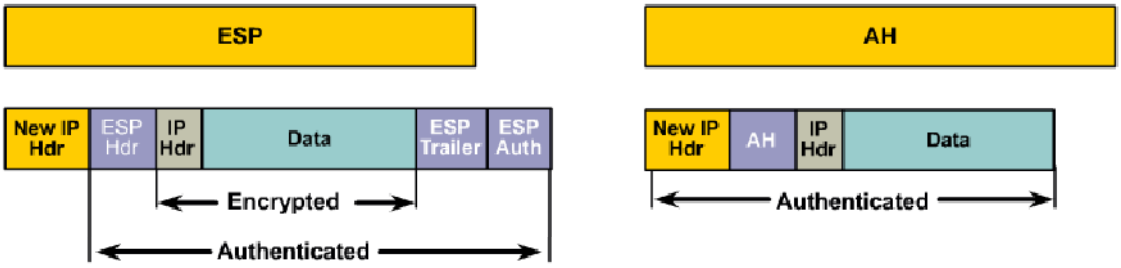
  1. Ustaví dvojcestný ISAKMP SA kanál mezi koncovými body pro zajištění bezpečného řídícího spojení.

2. Xauth – uživatel zasílá autentizační údaje. Xauth je volitelná, proto se někdy neudává jako samostatná fáze.
3. Pro přenos dat jsou ustanoveny dva jednocestné IPSec SA kanály. Pro každý kanál se používá jiný klíč.

Je také možné se setkat pouze se dvěma fázemi, kdy Xauth je považována za 1,5. fázi.

Pro šifrovaní IPSec využívá několik šifrovacích algoritmů DES, 3DES, AES, atd. a pro autentizaci využívá např. algoritmy MD5 a SHA-1. Z tohoto důvodu IPSec používá dva druhy hlaviček (Obr. 7), které mohou být vzájemně zkombinovány:

- ESP hlavička umožňuje autentizaci a šifrování původního paketu,
- AH hlavička autentizuje celý paket včetně nové hlavičky, ale neumožňuje šifrování.

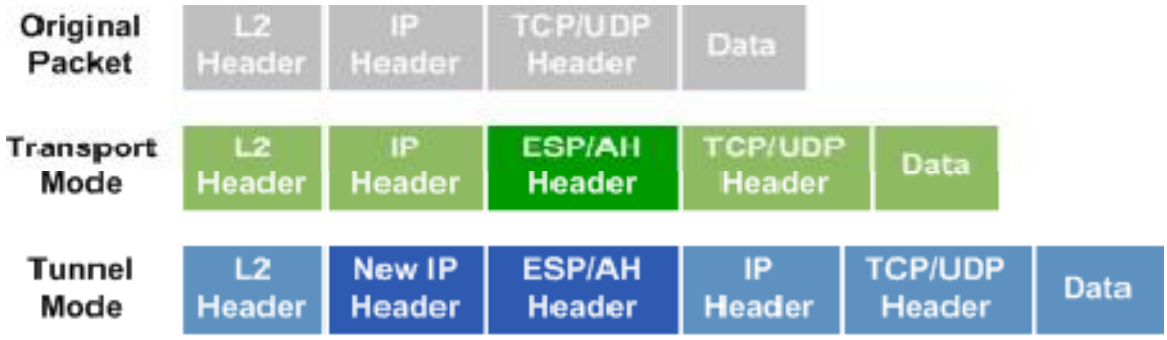


Obr. 7 IPSec hlavičky

IPSec VPN dokáže pracovat ve dvou modech – transportním nebo tunelovacím (Obr. 8).

- Transportní mód přidává jen ESP/AH hlavičku za původní IP hlavičku, nebo pracuje s GRE protokolem, který skryje adresu koncových stanic přidáním vlastní IP hlavičky. GRE je protokol, do kterého lze zapouzdřit jiný protokol. Toho se využívá např. pro tunel mezi směrovači.

- Tunel mód zapouzdří celý původní IP paket, a proto musí přidat vlastní novou IP hlavičku. V praxi se hlavně používá tento mód [13].



Obr. 8 Módy IPSec

Výhody IPSec VPN jsou:

- Je transparentní pro veškeré aplikace, protože pracuje na třetí vrstvě.
- Má relativně nízké nároky na výkon počítače a rychlost sítě.
- Je vhodný pro uživatele, kteří vyžadují plný přístup do sítě.
- Je vhodný pro L2L (LAN-to-LAN) VPN spojení.
- IPsec spojení je velmi bezpečné, jestliže je použit algoritmus AES a optimální časy pro výměnu klíčů.

IPSec má i několik nevýhod:

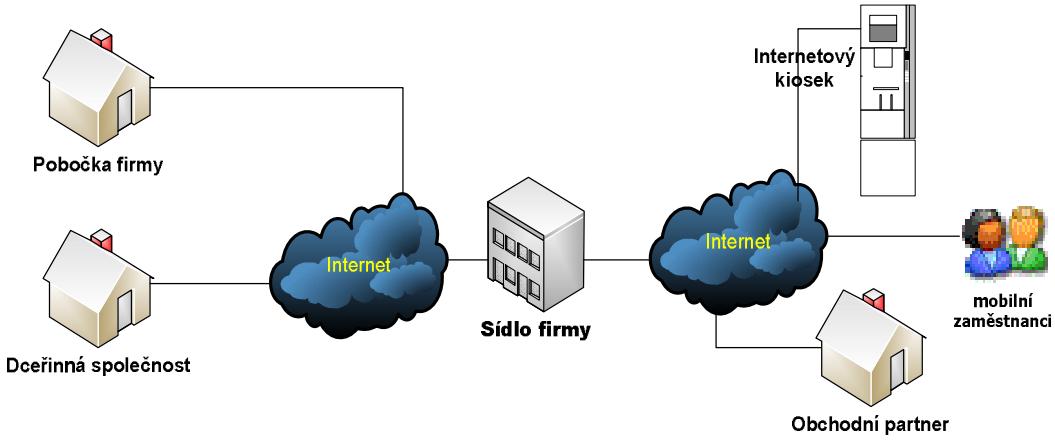
- IPSec VPN může mít problémy při přechodu přes NAT, nebo je protokol zakázaný na FW. Blokování protokolu IPSec na FW se vyskytuje stále častěji z důvodu snahy některých zemí monitorovat a omezovat internet. To má za následek, že z některých veřejných míst nelze používat IPsec VPN.
- Uživatel má přístup vždy do celé LAN sítě, což není vhodné pro externí pracovníky dané firmy a omezení pro ně se musí provádět na firewallech.

3.3.4 SSL VPN

Technologie SSL (Secure Sockets Layer) byla vyvinuta roku 1994 firmou Netscape pro bezpečnou komunikaci mezi webovým prohlížečem a serverem. Později firma zanikla.

Během let protokol SSL prošel několika verzemi až po dnešní TLS 1.2 (Transport Layer Security) a byla opravena řada nedostatků. Dnes je možné technologii SSL s protokolem TLS použít pro zabezpečení jinak vůbec nezabezpečených protokolů, jako je Telnet nebo FTP. SSL umí také vytvořit tunel podobně jako IPSec, ale je výpočetně náročnější, protože používá asymetrické šifrování založené na certifikátech a většinou se neobejde bez hardwarového akcelerátoru. Většina klientů podporujících SSL VPN používá pro zpřístupnění celé domovské sítě IPSec protokol a v případě, že ten selže, protokol SSL VPN.

Mezi IPSec a SSL je několik podstatných rozdílů (Obr. 9). Zatímco IPSec zpřístupňuje celou síť, SSL VPN zpřístupňuje jen určité porty. Je tedy zaměřena více na aplikace, což umožňuje podrobně nastavit, ke kterým servisům má vzdálený uživatel oprávnění přistupovat. V případě IPSec se musí také řešit uživatelova stanice z hlediska bezpečnosti, u SSL ověřování bezpečnosti stanice není nutné [14].



IPSec	
Typ spojení	pevné
Druh spojení	network
Druh kontroly	IP kontrola
Síťová bezpečnost	bezpečný zdroj a cíl
Vhodné užití	spojení vzdálených poboček s centrem spojení firemních počítačů s centrem

SSLVPN	
Typ spojení	pevné nebo mobilní
Druh spojení	aplikační přístup
Druh kontroly	uživatel / aplikační kontrola
Síťová bezpečnost	bezpečný i nebezpečný zdroj
Vhodné užití	mobilní uživatele, internet kavárny, obchodní partneři, spojení LAN to LAN

Obr. 9 Rozdíly mezi IPSec a SSL VPN

SSL VPN zařízení většinou pracují ve třech režimech.

- Core Access (Základní připojení) umožňuje přístup k webovým službám jen za použití webového prohlížeče a podporuje protokoly pro vzdálený přístup jako jsou RDP, Telnet, Citrix, SSH. Jeho použití je multi platformní, protože vyžaduje jen prohlížeč podporující SSL VPN. V tomto modu nelze využívat klient/server aplikace a vyskytují se problémy s webovými aplikacemi napsanými v Adobe Flash.
- Application Layer Access (Připojení pro aplikace klient/server) – je nutné nainstalovat ActiveX komponent pro platformu Windows, pro ostatní platformy JAVA klienta. V tomto režimu SSL VPN pracuje podobně jako proxy firewall. SSL VPN zařízení se pro aplikačního klienta tváří jako server a pro server jako aplikační klient. SSL VPN zařízení monitoruje a překládá provoz mezi skutečným aplikačním klientem a serverem.
- Network Connect (Síťové spojení) pracuje podobně jako IPSec VPN a vyžaduje instalaci klienta [15].

3.3.5 Wireless připojování

Bezpečnost připojování v klasických (drátových) sítích je dosti vysoká, přestože se jedná o komplikovanou záležitost. Může se omezit MAC adresa směrovačů, přepínačů a jiných síťových komponentů. Pro bezpečnější provoz lze také nastavit virtuální lokální síť nebo VPN.

U bezdrátových sítí se bezpečnost stává komplikovanější. Rozebírání paketů a jejich bezdrátové přesouvání znamená, že každý, kdo je v dosahu, je může číst. Útočník s dobrou směrovou anténou může bezdrátovou síť pasivně monitorovat, a přitom být daleko od přístupového bodu (AP – Access Point). Po celou dobu monitorování nemůže být odhalen správci sítě. Níže uvedu možnosti zabezpečení bezdrátové sítě.

3.3.5.1 Wired Equivalent Privacy – WEP

IEEE specifikace pro 802.11 a/b/g nabízí hlavně šifrování zvané WEP, které je založeno na RC4 algoritmu. Je zde používán 40 bitový kódový klíč. Každý, kdo zná tento tajný klíč, se může zúčastnit provozu na WEP síti. Tajný klíč se obvykle skládá z řetězce písmen, číslic a speciálních znaků nebo poněkud delšího řetězce hexadecimálních čísel.

WEP má dvě nevýhody:

1) WEP síť komunikuje šifrovaně, kdežto na AP jsou všechny pakety dešifrovány a posílány do klasické sítě v čisté podobě.

2) Ostatní počítače zapojené do klasické sítě znají také tajný klíč pro WEP síť a mohou číst všechny přijaté a poslané pakety.

WEP se ujal malých a středních sítí a považuje se jen za první linii obrany. Jestliže se správce sítě obává útoku cíleně zaměřeného na jeho síť, musí používat efektivnější zabezpečovací systémy [16].

3.3.5.2 Standard 802.11i

Standard 802.11i nabízí reálnou bezdrátovou bezpečnost a silný šifrovací systém. Pracovat na tomto standardu se začalo roku 2001, bohužel práce neprobíhaly tak rychle, jak se očekávalo a z tohoto důvodu se v polovině roku 2002 Wi-Fi aliance a konsorcium výrobců spojily a navrhly bezdrátový bezpečný přístup - WPA (Wireless Protected Access). WPA se tak stala podmnožinou standardu 802.11i a začlenila zde dva hlavní rysy:

- používání autentizačního protokolu 802.1x,
- používání dočasného klíče.

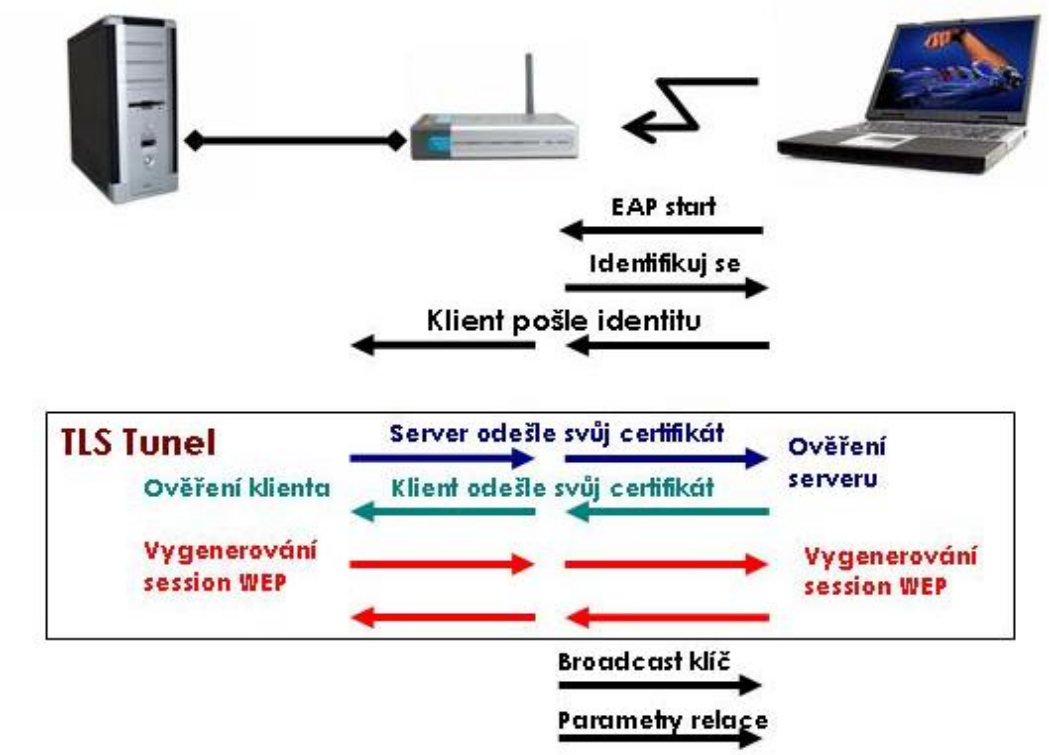
3.3.5.3 Autentizační protokol 802.1x

Tento protokol byl původně navržen pro klasickou síť. Je to autentizační mechanismus, který pracuje na základě portu. Když se chce klient autentizovat, provoz je povolen přes

port klienta skrz autentizační zařízení do chráněné sítě. V bezdrátové síti se tento princip uchoval. Klient se musí autentizovat vůči AP, jestliže k tomu nedojde, není mu dovoleno do chráněné sítě vstoupit.

Protokol 802.1x používá čtyři části procesu autentizace (Obr. 10):

- suplikant (program běžící u klienta) kontaktuje autentizátor (AP),
- autentizátor žádá pověření od suplikanta a toto pověření zkontroluje autentizační serverem,
- autentizační server ověřuje suplikanta jménem autentizátora,
- jestliže je suplikant autentizován, přístup je mu udělen.



Obr. 10 Průběh autentizace u bezdrátového spojení

Dříve, než autentizace proběhne, se veškerá komunikace realizuje přes nechráněný port. Po autentizaci je používán port chráněný. Pro autentizaci mezi autentizátorem

a suplikantem se používá EAP protokol (Extensible Authentication Protocol). Existuje mnoho variant tohoto protokolu. Zde jsou uvedeny některé z nich:

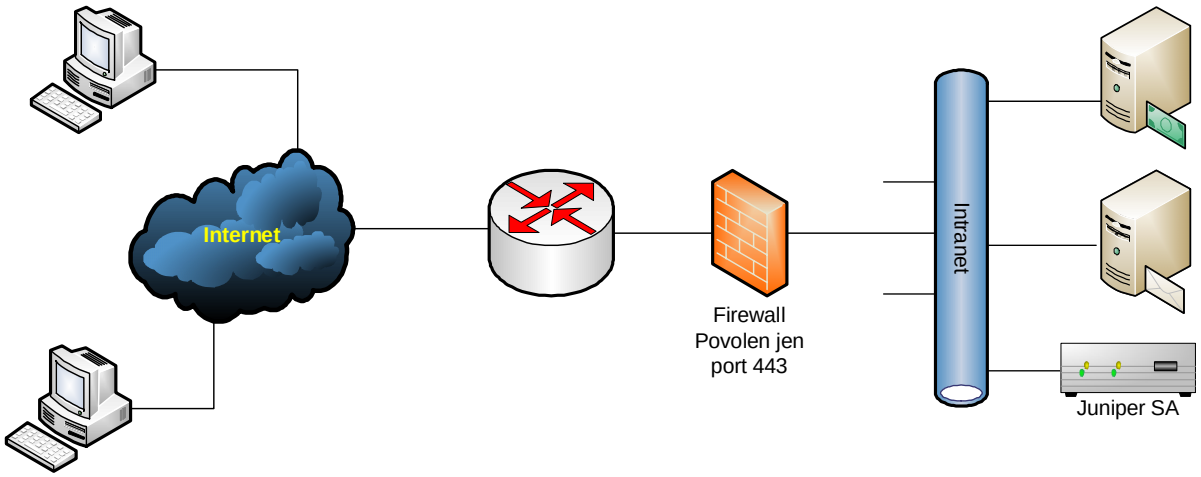
- EAP-MD5 – tento protokol využívá metodu výzvy a odpovědi. Tento protokol nedovoluje vzájemnou autentizaci.
- EAP-TLS – pracuje na bázi digitální certifikace a stal se nejpoužívanějším protokolem pro bezpečnou bezdrátovou síťovou komunikaci. Tento protokol nicméně vyžaduje používání veřejného klíče, který nelze dost dobře implementovat do malých sítí.
- PEAP – byl nabízen jako alternativa k protokolu EAP-TLS. Tento protokol používá server-certifikát, který také umožňuje serveru autentizovat se vůči suplikantovi. Vytváří EAP-TLS tunel, ve kterém se pak používají ostatní autentizační metody, např. MD5.
- EAP-TTLS – pracuje podobně jako PEAP, vytváří tunel mezi suplikantem a RADIUS serverem a podporuje ostatní metody EAP (MD5, MS-CHAP).
- LEAP – ciscová verze EAP, která pracuje většinou pouze s cisco bezdrátovými kartami [17].

4 Praktická část

Technologii SSL VPN a její konfiguraci popíši na zařízení Juniper Network Secure Access SA 6500. Juniper SA od této společnosti v oblasti vzdáleného připojování patří mezi světová špičková zařízení. Společnost Juniper Networks, Inc. vyrábí Juniper Secure Access zařízení ve čtyřech řadách. Nejnižší řada SA 700 je určena pro malé a střední firmy. Zařízení umožňuje práci jen v základním režimu (Core Access) a je schopno obsloužit najednou až 25 uživatelů. Řada SA 2000 již dovoluje využívat všechny tři SSL VPN režimy, dokáže obsluhovat až 100 uživatelů a má implementovanou funkci pro bezpečné vytvoření konferencí (Secure Meeting). Zařízení je již možné zapojit do clusteru. Vyšší řada SA 4000 obsluhuje najednou až 1000 uživatelů, navíc má centrální spravování a umožňuje nakonfigurovat dvě bezpečnostní cesty (Two Arms System). Nejvyšší řada SA 6000 již obsluhuje až 3000 uživatelů najednou a navíc lze několik zařízení zapojit do Multi clusteringu.

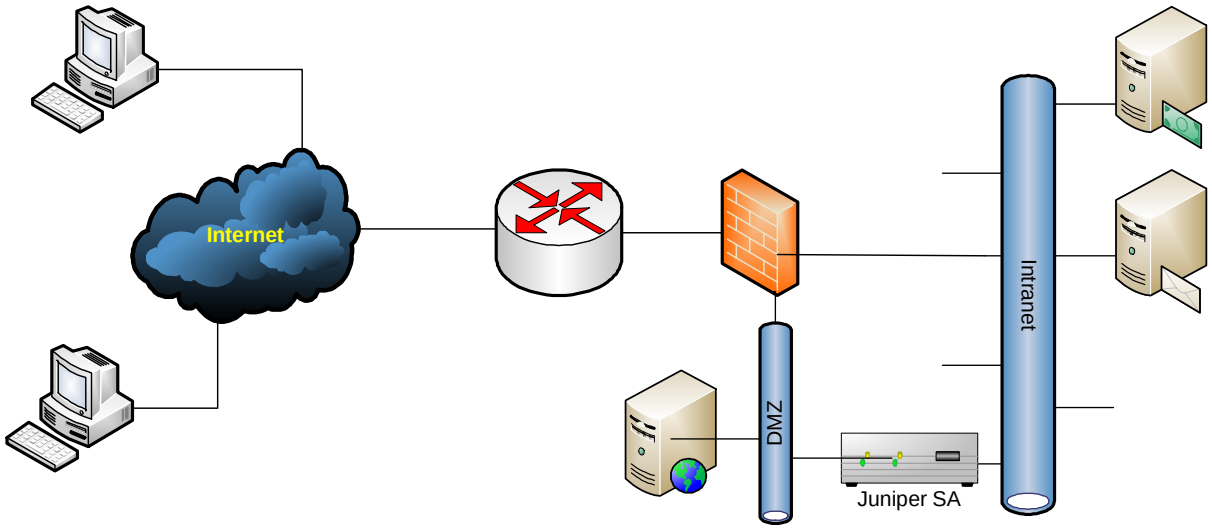
Výše jsem se zmínil o jednom způsobu napojení Juniper SA zařízení do sítě, tzv. Two Arms System. Juniper SA zařízení se zapojují třemi způsoby.

- One Arm, no DMZ (Jedna bezpečnostní cesta, bez DMZ). Jedná se o jednoduché a efektivní zapojení Juniper SA zařízení do interní sítě. Firewall je nakonfigurován tak, že povoluje jen SSL provoz (port 443) na Juniper SA zařízení, ostatní provoz je zahazován (Obr. 11).



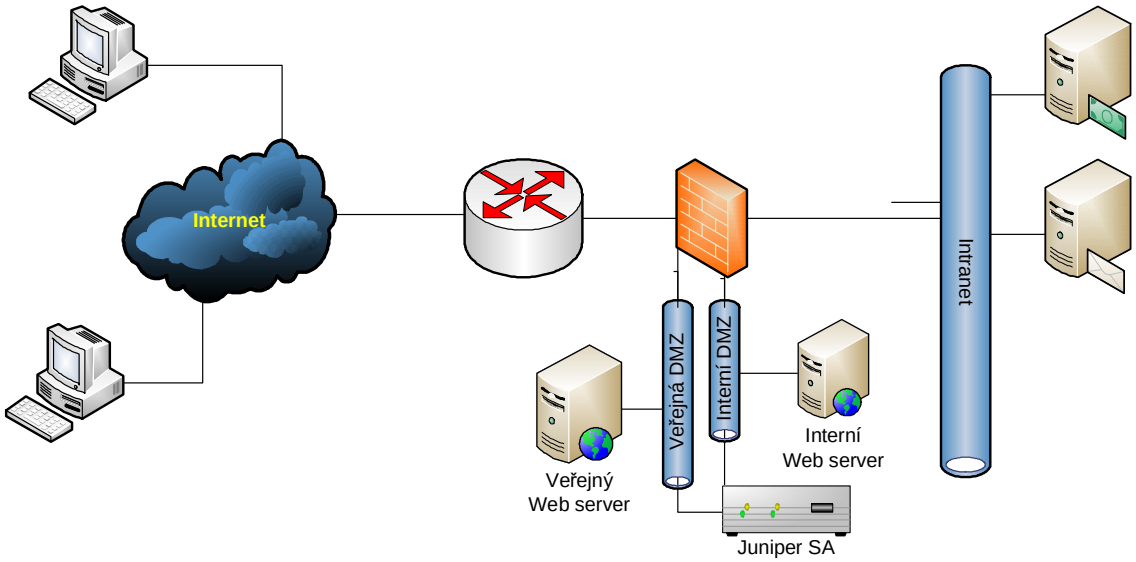
Obr. 11 Zapojení One Arm, no DMZ

- Two Arms, DMZ (Dvě bezpečnostní cesty, DMZ). Jestliže je v síti DMZ zóna, je možné využít toto zapojení. Externí rozhraní Juniper SA zařízení je napojeno na DMZ zónu a interní rozhraní do interní sítě. Firewall je nakonfigurován tak, aby provoz do interní sítě směroval na Juniper SA zařízení a zařízení převádí provoz do interní sítě, pracuje podobně jako proxy firewall (Obr. 12).



Obr. 12 Zapojení Two Arms, DMZ

- Two Arms, Two DMZ (Dvě bezpečnostní cesty, dvě DMZ) je možné vytvořit dvě DMZ zóny s rozdílnou bezpečnostní úrovní. V úrovni s nižší bezpečností bude umístěn server poskytující veřejné služby, např. veřejný webový server. V Druhé DMZ zóně je umístěno Juniper SA zařízení a např. interní web server. Juniper SA zařízení má externí rozhraní připojeno do veřejné DMZ a interní rozhraní do interní DMZ. Firewall směřuje provoz, který míří do interní sítě na Juniper SA zařízení a zařízení převádí provoz do interní sítě. Provoz je opět směrovaný přes další firewall (Obr. 13) [15].



Obr. 13 Zapojení Two Arms, Two DMZ

4.1 *Konfigurace Juniperu SA6500*

Při zavádění Juniper SA zařízení do provozu je nutné dobře navrhnout bezpečnostní politiky, které se budou aplikovat na jednotlivé skupiny uživatelů. Je možné nastavit bezpečnostní politiky přímo na uživatele, ale nastavení politik na uživatele přináší velké problémy při spravování zařízení. Při každé změně pozice zaměstnance se musí politiky složitě upravovat. Při uplatňování politik na skupiny stačí pak zaměstnance přesunout do jiné skupiny. Velmi často se databáze uživatelů a skupin propojují s jinými systémy, např. s Active Directory.

Je velmi žádoucí konfiguraci skupin zdokumentovat. Dokumentace by měla obsahovat tyto parametry:

- Role
- Autentizační metody
- Zmapování bezpečnostních pravidel na role
- Autentizační realmy
- Přístupová pravidla

4.1.1 Inicializační konfigurace SA 6500

Pro první konfiguraci se používá sériový port s následujícími parametry: 9600 baund; 8 data bits; 1stop bit; No flow control. V inicializačním programu se zařízení ptá, jestli bude pracovat samostatně nebo v clusteru (Obr. 14).

```
Starting system software version 6.0R2 (build 11509)

About to boot as a stand-alone IVE.
Hit TAB for clustering options, wait or hit Enter for continue...
Starting Core Services

Welcome to the initial configuration of your server!
NOTE: Press 'y' if this is stand-alone server or first machine in
clustered configuration
If this is going to be a member of an already running cluster
press 'n' to reboot. When you see the 'Hit TAB for clustering
options' message press TAB and follow the directions.
Would you like to proceed (y/n):_
```

Obr.14 Konfigurační dialog 1

V dalším kroku se program ptá na licenční podmínky. Pro přečtení licenčních podmínek je nutné vložit „r“, při nesouhlasu s licenčními podmínkami a stlačením písmene „n“ se konfigurační program ukončí. Pro pokračování je nutné stlačit „y“ (Obr. 15).

```
Note that continuing signifies that you accept the terms of the
Juniper License agreement. Type 'r' to read the license agreement
(the text is also available at any time from the license tab in
the Administrator Console).
Do you agree to the terms of the license agreement (y/n/r)?:
```

Obr. 15 Konfigurační dialog 2

Následuje síťové nastavení Juniper SA zařízení, kde se nastavují následující parametry

```
Please provide ethernet configuration information
  IP address:         10.0.0.100
  Network mask:       255.255.0.0
  Default gateway:    10.0.0.1
Please provide DNS nameserver information
  Primary DNS server: 4.4.4.4
  Secondary (optional):
  DNS domain(s): pixla.net
Please provide Microsoft WINS server information:
  WINS server (optional):

Please confirm the following setup:
  IP address:         10.0.0.100
  Network mask:       255.255.0.0
  Default gateway:    10.0.0.1
  Link speed:         auto
  Primary DNS server: 4.4.4.4
  Secondary (optional):
  DNS domain(s): pixla.net
  WINS server (optional):
Correct? (y/n): y
```

(Obr. 16).

Obr. 16 Konfigurační dialog 3

V následujícím kroku se vytváří účet lokálního administrátora pro přístup ze sériové konzoly. Pro větší bezpečnost je vhodné nepoužívat jméno Admin nebo Administrátor

```
-----------------------------------

Please create an administrator username and password.
  Admin username:     Bambula
  Password:
  Confirm Password:

The administrator was successfully created.

-----------------------------------
```

(Obr. 17).

Obr. 17 Konfigurační dialog 4

Administrátorský účet je vytvořen v lokální autentizační databázi na Juniper SA zařízení. Později se může vytvořit externí administrátorský účet pro přístup přes webové rozhraní.

Lokální administrátorský účet je důležitý pro přístup na zařízení v případě, že je zařízení nedostupné po síti.

V předposledním kroku inicializačního konfiguračního programu se vytváří „Self – Signed“ digitální certifikát, který je zařízením používán pro SSL spojení. Pro digitální vytvoření certifikátu je nutné zadat jeho jméno a jméno organizace. Náhodné znaky slouží jako jádro pro vytvoření veřejného a privátního klíče asymetrické šifry (Obr. 18).

Po ukončení inicializačního programu systém uloží nastavení a zobrazí na konzole menu, které umožní změnit jednotlivé parametry nastavení včetně defaultního – je zde možné nastavení log systému a možnost ukládání logů. Menu je dostupné jen z lokálního administrátorského účtu.

```
Please provide information to create a self-signed Web server
digital certificate.
  Common name (example: secure.company.com): agent007.pixla.net
  Organization name (example: Company Inc.): Pixla s r.o.

Please enter some random characters to augment the system's random
key generator. We recommend that you enter approximately thirty
characters.

Random text (hit enter when done):
asdikmt56.86(hjnftsdsniklkuyf6798akjidr!'ksjdyxj87

Creating self-signed digital certificate...
The self-signed digital certificate was successfully created.

------------------------------------
Congratulations! You have successfully completed the initial set
up of your server.
```

Obr. 18 Konfigurační dialog 5

4.1.2 Konfigurace přes webové rozhraní

Po základní konfiguraci se již další nastavení provádí přes webové rozhraní. Pro přihlášení se používá protokol „https“, jako URL adresu pro administrátorské přihlášení je nutné za IP nebo jméno Juniper SA zařízení připsat lomítko a slovo admin. např.: `https://agent007.pixla.net/admin`. Při prvním přihlášení se objeví upozornění na to, že certifikát není vydán všeobecně známou certifikační autoritou. Protože jsme si certifikát vytvořili sami, tak si ho můžeme sami schválit.

Jakmile přidáme nové zařízení, pravděpodobně nebude nainstalována poslední verze Firmware, který Juniper nazývá „JUNOS“. Proto prvním krokem administrátora bude povýšit JUNOS na poslední verzi. Poslední verzi JUNOSu je možné najít na stránkách

společnosti Juniper Network[6]. Pro přihlášení musí být uživatel registrován na těchto stránkách.

Webové rozhraní má i základního průvodce pro konfigurovaní. Průvodce již předpokládá základní dovednosti s Juniper SA zařízeními v rozsahu CJSA školení.

4.1.2.1 Uživatelské role

Každý uživatel musí být přiřazen k jedné nebo více rolí. Role je entita, pro kterou se definují následující parametry:

- určení typu servisu (SSH, Telnet, web, aplikace, soubory, meeting, email, network a terminál),
- linky ke zdrojům na přístupové stránce,
- nastavení uživatele na rozhraní,
- uživatelova relační nastavení a volby.

Vytváření role se uskuteční z hlavního menu přes záložku „User Roles“, vybere se „New Role“, vloží se jméno a popis role. Popisy usnadňují pozdější orientaci v rolích. Po vytvoření role je nutné povolit potřebné servisy pro uživatele. V třetím kroku se pak definují tzv. „Bookmarks“, tedy linky které se uživateli zobrazí. V posledním kroku se povolují další relace, jako např. povolení ZIP komprese, Java apletů, atd. Na obrázku jsem ukázal některé nadefinované role včetně povolených parametrů (Obr. 19).

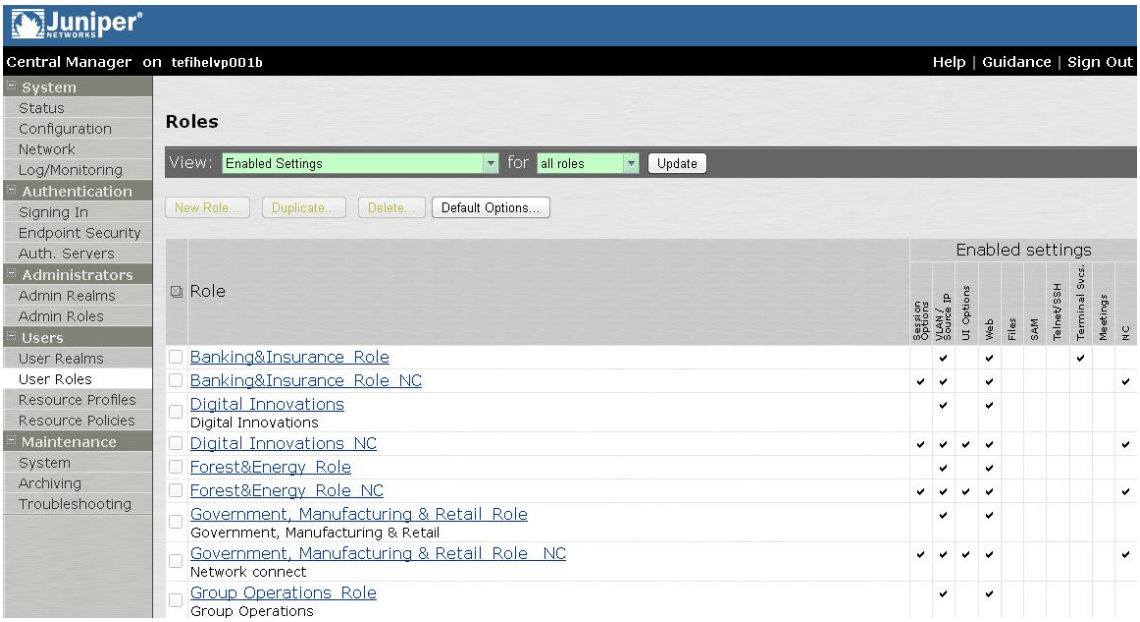
Po uložení nové role se na horní liště objeví několik nových záložek. V záložce Web pak přidáváme jednotlivé odkazy – „Bookmark“. Pro vytvoření nového bookmarku je nutné zadat jeho jméno a odkaz na stránku.

Jsou zde další možnosti nastavení, např.:

- Zda se má odkaz otevřít v novém okně, nebo přepsat stávající.
- Zda je přístup povolen jen na danou URL adresu a další odkazy jsou blokovány, popřípadě je možné povolit i odkazy vyskytující se na povolené stránce.

[6] www.juniper.net/support

- Zda povolit java aplet.
- Po jakém čase nečinnosti se spojení ukončí.
- Jaká je maximální doba spojení, atd.

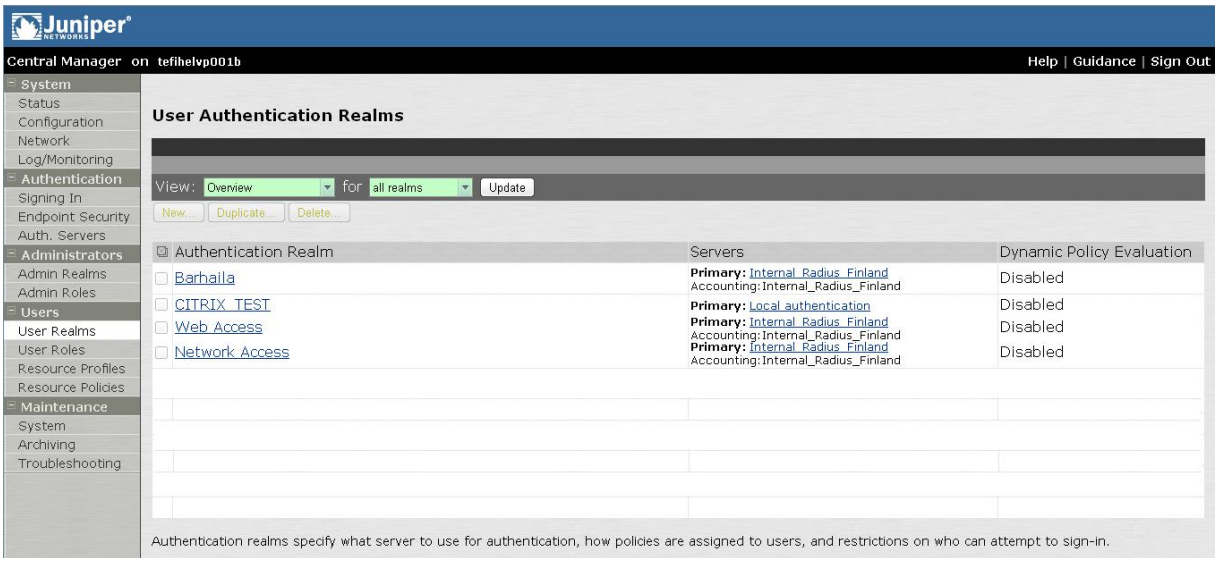


Obr. 19 Nastavení rolí

4.1.2.2 Uživatelské realmy

Jakmile jsou role definovány, musí se namapovat na uživatele a nastavit pravidla, která jsou součástí nastavení realmů. Pravidla se vytvářejí pod záložkou „User Realms“, přejde se na záložku „Role Mapping“ a stlačí se tlačítko „New Rule“. V okně pro vytváření pravidel se vybere uživatel, vybere se role a nastaví kriteria. Pravidel pro uživatele se může nastavit více a záleží na pořadí, ve kterém jsou pravidla uspořádána. Pravidla se aplikují shora dolů a jestli již nějaké pravidlo nějaký servis zakáže, na pozdější pravidlo již nebude brán zřetel.

V realmech se také nastavuje způsob autentizace, a který autentizační server má přednost. Jestliže je dostupný primární autentizační server sekundární se již neuplatní. Pokud je tedy např. primární RADIUS server a sekundární lokální autentizace, pak se uživatel (i administrátor) musí přihlásit účtem z RADIUS serveru. Lokální autentizace se uplatní tehdy, jestliže je RADIUS server nedostupný (Obr. 20).



Obr. 20 Způsob autentizace

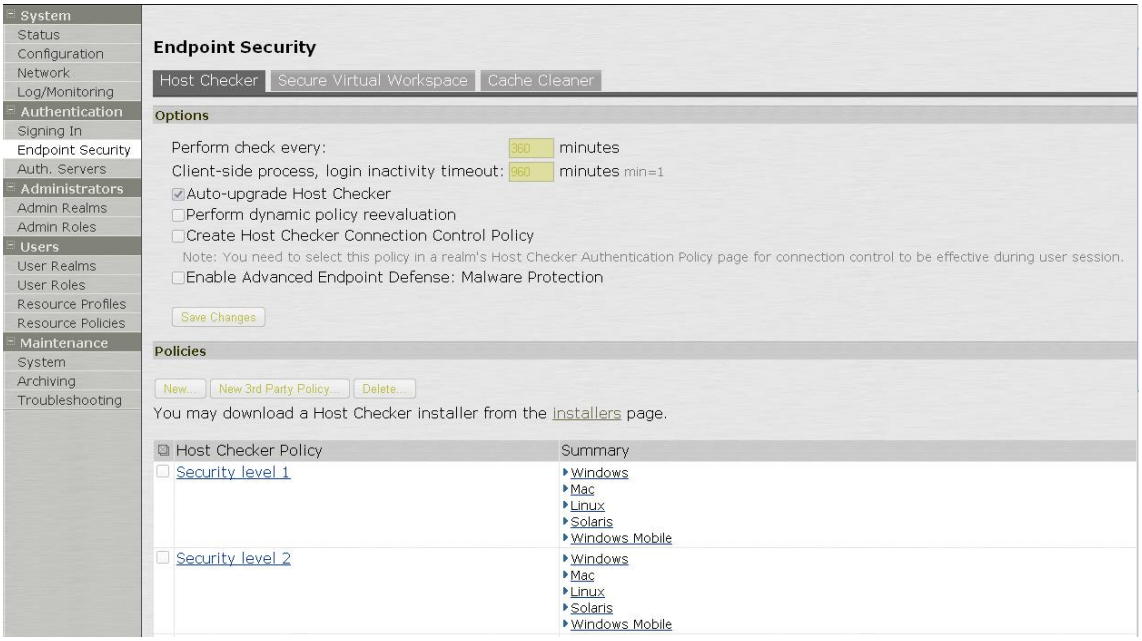
4.1.2.3 Nastavení vyžadovaných pravidel

Pro různé přihlašovací režimy můžeme nastavit vyžadovaná pravidla, např. který prohlížeč je povolen a podobně. Tato pravidla se hlavně nastavují pro Network Connect, protože ten povoluje přístup do celé sítě. Ve firmě, byla nastavena následující pravidla.

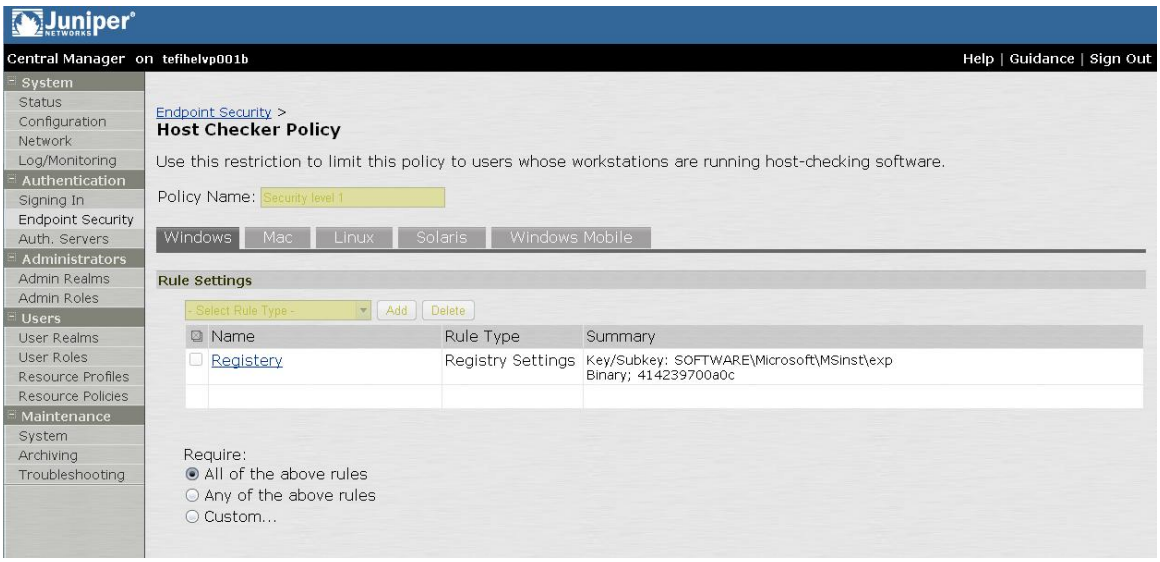
- Pro režim „Network Connect“ musí být na stanici nainstalován „Juniper Network Connect“ klient. Tento klient se automaticky instaluje při přihlášení na úvodní webovou stránku, jakmile je vybrán tento režim.
- Security pravidlo 1 vyžaduje na stanici instalaci firemního operačního systému a kontroluje určité klíče v registrech.
- Security pravidlo 2 kontroluje, zda je zapnut správný antivirový program (Obr. 21, Obr. 22).

Pro kontrolu pravidel se při prvním přihlášení nainstaluje na stanici aplikace „Host Checker“, která kontroluje vyžadovaná pravidla, a to v průběhu spojení. Např. kdyby

uživatel vypnul antivirový program po úspěšném navázaní spojení, host checker by to zjistil a okamžitě by přerušil spojení.

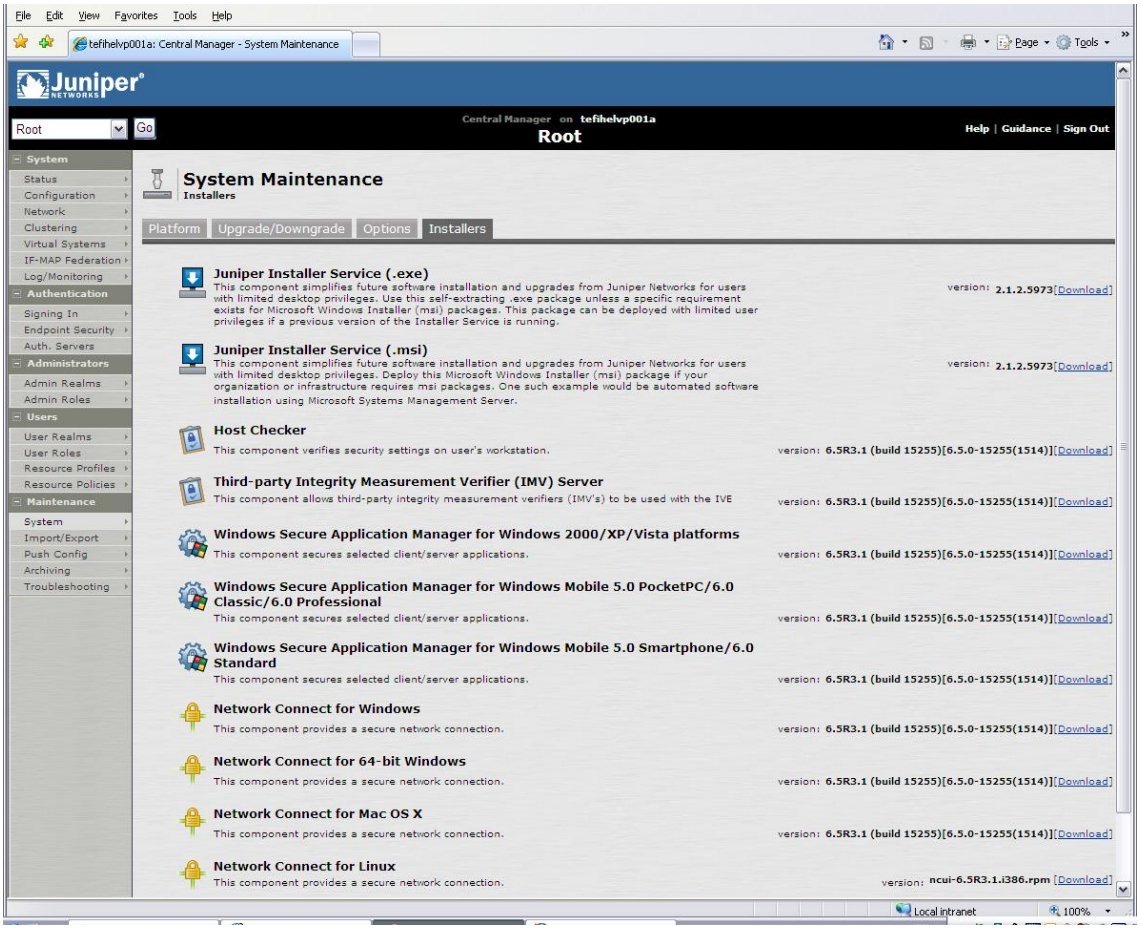


Obr. 22 Pravidla pro stanice



Obr. 23 Kontrola klíče v registrech

Host checker se instaluje z Juniper SA installeru. Zde již jsou umístěny aplikace pro instalování a v pravidlech se určuje, kdy a jaká aplikace se na stanici instaluje (Obr. 23).



Obr. 23 Juniper SA Installer

4.1.2.4 Nastavení Host Checkeru

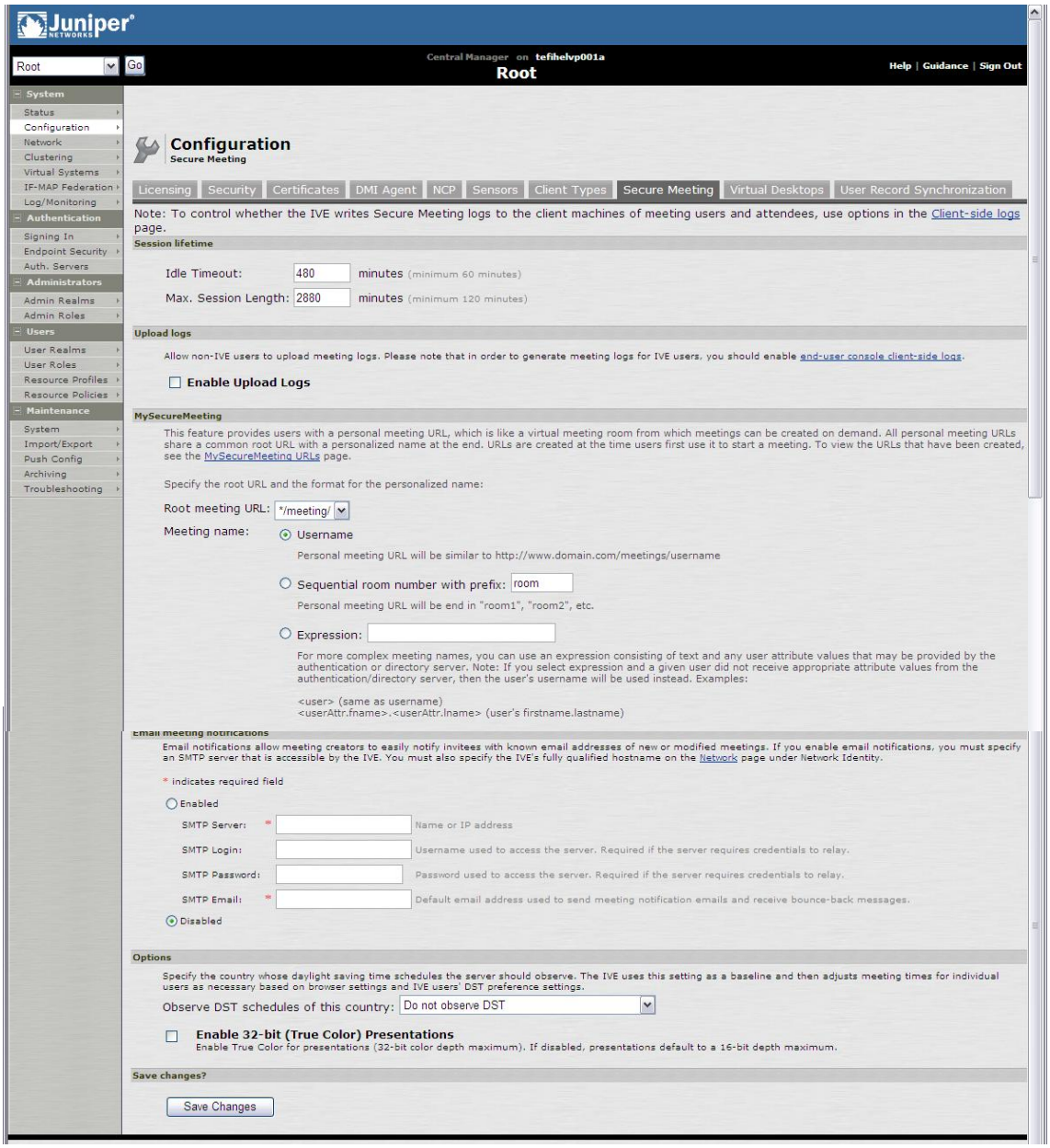
Výše jsem zmínil funkci „Host Checkeru“ a z předchozího je patrný velký bezpečnostní význam této aplikace, která je součástí Juniper SA zařízení. Nastavení Host Checkeru se provádí pod záložkou "Endpoint Security" v záložce "Host Checker". Důležitým parametrem Host Checkeru je interval kontroly nastavených pravidel. Nastavení intervalu na 0 má za následek, že se kontrola stanice provede jen při prvním přihlášení. Nastavuje se zde také to, zda se má na stanici nainstalovat vždy poslední verze Host Checkeru. Host Checker rovněž může kontrolovat útok na stanici z jiné stanice ve stejné

LAN, i když stanice zrovna není napojena na Juniper SA. Host checker je také schopen hlídat update antivirových databází a automaticky stahovat poslední verze. Host Checker má předdefinované některé funkce, např. kontrolu firewallů a antivirových programů na stanicích, ale mnoho dalších pravidel si můžeme nastavit sami. Nastavená pravidla mohou být vyžadována všechna nebo jen některá.[7]

4.1.2.5 Nastavení virtuální konference (meeting)

Velmi příjemnou Juniper SA funkcí je nastavení bezpečné virtuální konference, které se mohou zúčastnit ověření uživatelé. Ve virtuální konferenci je možné sdílet data, posílat e-maily, provádět prezentace, atd. Tato funkce se může zdát nadbytečná, protože podobné služby mají i jiné platformy, např. ciscoconference nebo MS Communicator Live Meeting. Pokud se ale do firmy pořizuje podobné bezpečnostní zařízení, a troufnu si říci, že žádná větší firma se bez dobrého zabezpečení neobejde, proč investovat do podobných systémů, když Juniper má již tuto možnost implementovanou. Navíc se lze po autentizaci přihlásit na virtuální konferenci přímo z přihlašovací stránky. Dále je vhodné omezit množství používaných aplikací, neboť se většinou jedná o další hesla, která je nutné si zapamatovat. Množství hesel vede k vytváření různých textových souborů s hesly a většinou jsou tyto soubory umístěny přímo na ploše, což představuje bezpečnostní riziko. Základní nastavení parametrů virtuální konference je na obrázku (Obr. 24).

[7] Logické funkce mezi pravidly „And“, nebo „Or“



Obr. 24 Nastavení virtuální konference

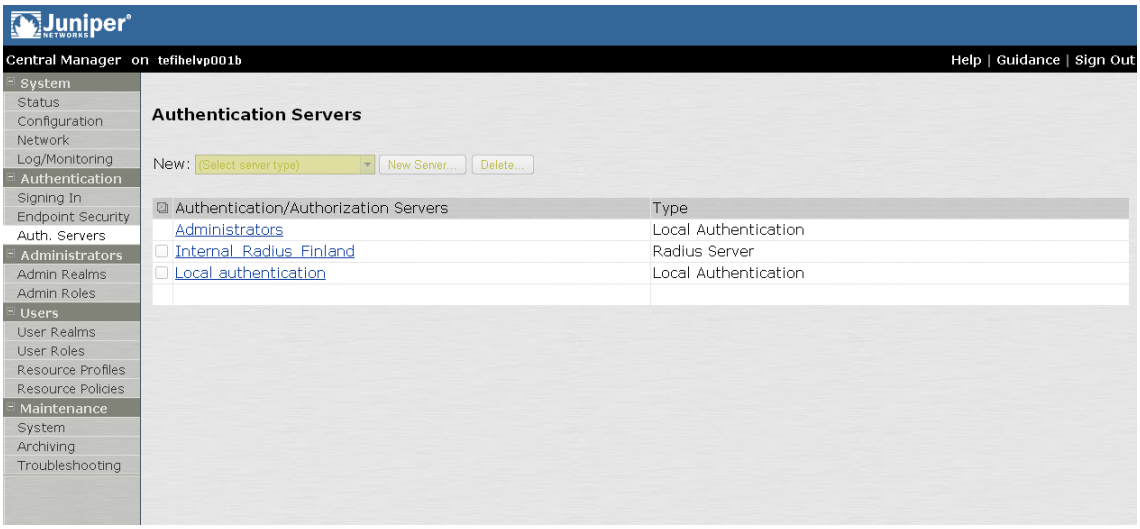
4.1.2.6 Nastavení autentizačních serverů

Jak jsem již zmínil v kapitole o realmech, je nutné nastavit i autentizační servery, protože nejlepším řešením není mít účty uživatelů uloženy v lokální databázi na zařízení Juniper SA. Pod záložkou „Auth. Servers“ se autentizační servery nastavují. Juniper SA

podporuje širokou paletu autentizačních serverů – lokální autentizační server, LDAP, NIS, ACE, RADIUS, Active Directory/NT, certifikáty, SAML, SiteMinder. Dále popíši nastavení lokálního autentizačního serveru a RADIUS serveru.

Lokální autentizační server musí mít zadáno jméno, nastaví se politika hesel, např. kolik znaků je minimum pro heslo, kdy vyprší atd. Tento autentizační server pak kontroluje údaje uživatele s údaji v lokální databázi uživatelů a hesel.

RADIUS server - je nutné nastavit zařízení Juniper SA jako RADIUS klienta a nastavit „Shared Secret“, což je řetězec znaků pro autentizaci RADIUS klienta RADIUS serverem.



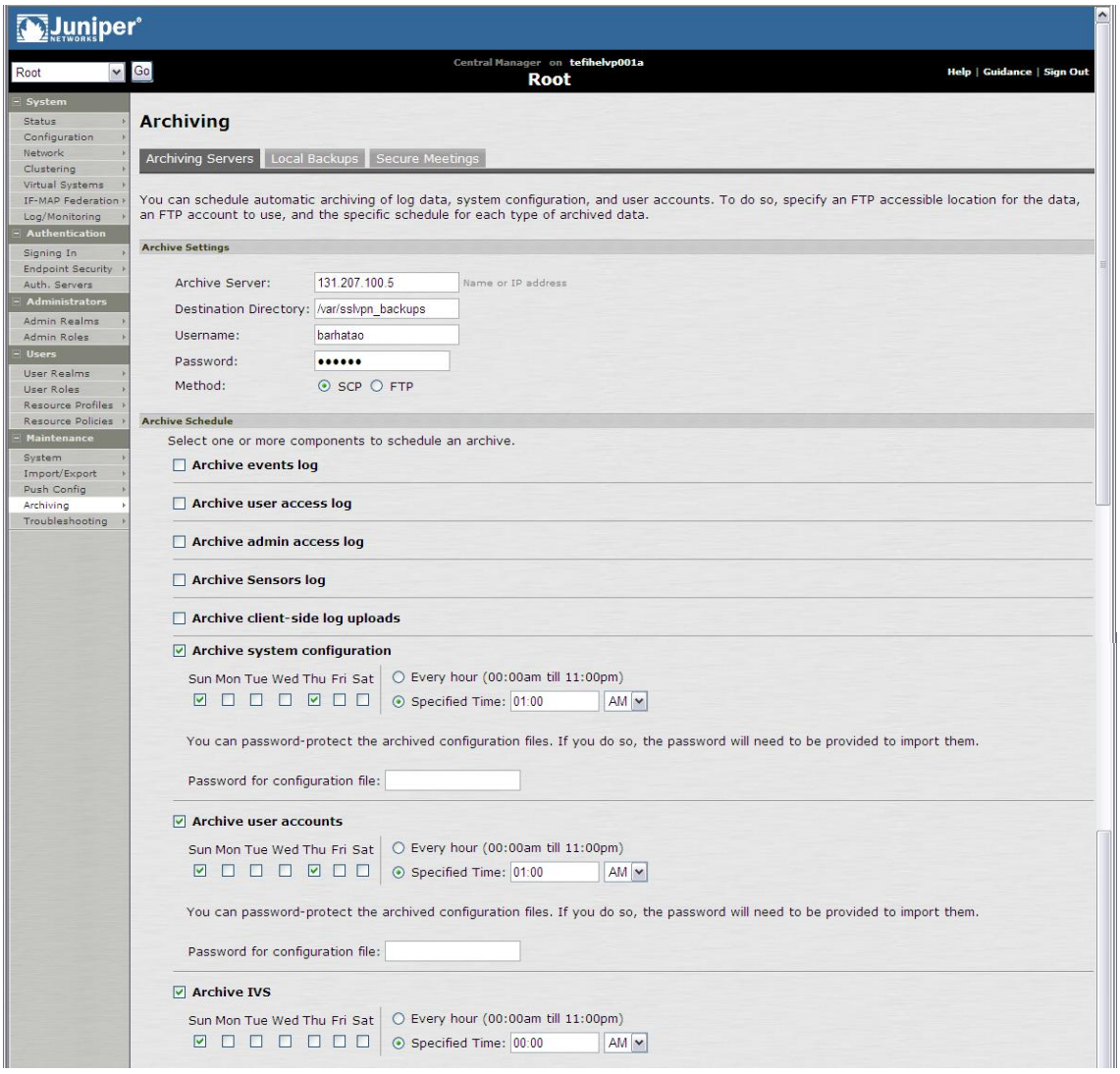
Obr. 25 Autentizační servery

4.1.2.7 Nastavení archivování

Archivování je možné nastavit na denní nebo týdenní režim. Systém může archivovat logy, nastavení a uživatelská jména a hesla (Obr. 26). Juniper SA používá při přenosu dat na archivovací server protokol ftp a veškerá odeslaná data šifruje. Jména archivních souborů uvádí tabulka (Tab. 2).

typ archivních dat	jméno souboru
System Events	JuniperAccessLog-date-time
User Events	JuniperEventsLog-date-time
Administrator Events	JuniperAdminLog-date-time
System Configuration Files	JuniperConf-date-time
User Accounts	JuniperUserAccounts-date-time

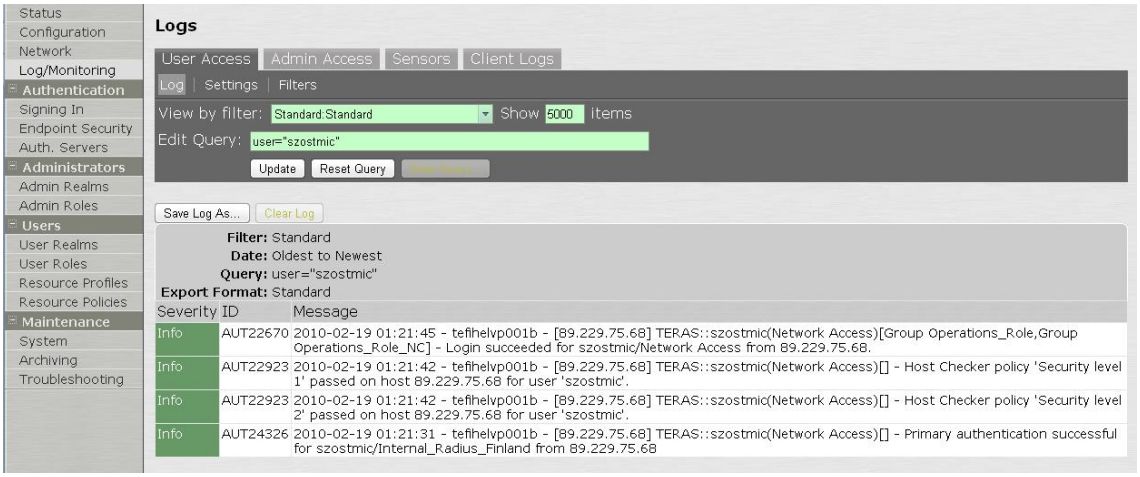
Tab. 2 Archivační soubory



Obr. 26 Nastavení archivace

4.2 *Provozní problémy SSL VPN na Juniperu SA6500*

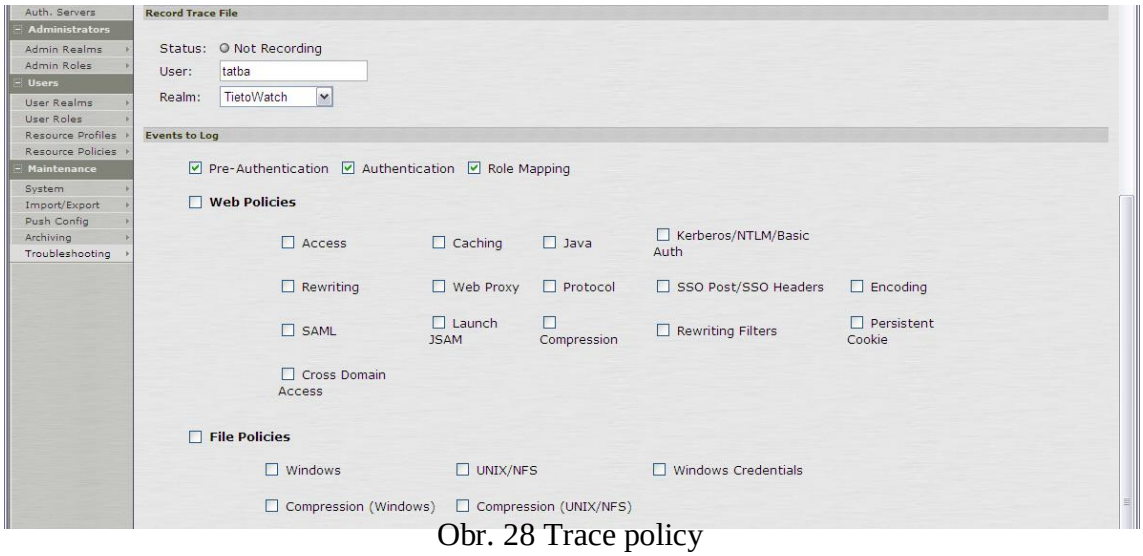
Juniper SA zaznamenává do „Events Log“ veškeré události jak v systému, tak v uživatelských relacích (Obr. 27). Je zde vidět, jak se uplatňovala jednotlivá pravidla na uživatele a proč byl uživatel odmítnut. Tyto logy by se měly kontrolovat při řešení problému jako první.



Obr. 27 Events Log

4.2.1 Záložka Troubleshooting

Zde se nachází funkce „Policy tracing“ (Obr. 28), která ukazuje jaká pravidla se aplikovala a proč se aplikovala. U této funkce je možné nastavit různé parametry podle toho, co přesně chceme zjistit.



Obr. 28 Trace policy

4.2.2 Problémy během pilotního provozu

Prvním problémem, který se objevil, bylo nestabilní připojení, které se vykytovalo nepravidelně. Po delším zkoumání se zjistilo, že vypadávání spojení nastává při připojení více než 300 uživatelů. Dalším šetřením se zjistilo, že předřazený firewall kapacitně nestíhá obsluhovat provoz. Musel se pořídit výkonnější firewall.

Dalším vážným problémem bylo uzamykání účtu při jednom špatném přihlášení. Zjistilo se, že příčinou je vyhledávač internet Explorer, který z neznámého důvodu posílá přihlašovací údaje několikrát po sobě. Tento problém zatím nebyl neodstraněn.

Host Checker neumožnil připojit se přes Network Connect. Problém byl odstraněn nainstalováním bezpečnostního balíčku pro Host Checker.

Problém s webovou aplikací pro správu mailů nastal při připojení uživatele přes webové rozhraní Juniper SA. Vyhledávání příčiny je velmi obtížné, protože se problém vyskytuje nepravidelně. Zatím ještě nebylo nalezeno řešení.

Jestliže se spojení přes network connect ukončilo nestandardně a v krátké chvíli se uživatel opět pokusil přihlásit, byla jeho relace odmítnuta. Příčinou je neukončení původní relace. Původní relace se udržuje funkční ještě několik minut, protože tím se zamezuje přerušení spojení při krátkém výpadku sítě. Jediné řešení je ukončit relaci standardním způsobem, nebo po nestandardním odpojení vyčkat několik minut a pak zahájit novou relaci.

Starší verze klientské aplikace Juniper Network Connect se nepravidelně zasekávala. Jakmile klient nahlásil chybu spojení, již se nepodařilo s ním opět připojit. Řešením bylo odinstalovat klienta a nainstalovat ho znovu. Problém se řešil se zákaznickým střediskem Juniperu a zcela vymizel s instalováním novější verze klientské aplikace. Pro jistotu byla původní verze odinstalována a poté nainstalována nová. Nebylo doporučeno povýšit starou verzi na novou.

5 Závěr

V teoretické časti diplomové práce jsem se snažil podívat na problematiku bezpečnosti IT systému v širším smyslu slova. Poukazuji na to, že není možné nahlížet na bezpečnost jen z jednoho úhlu pohledu. Dobré zabezpečení je komplex dílčích bezpečnostních opatření, která na sebe navazují a vzájemně se doplňují. Společnost, snažící se o dobré zabezpečení, by měla mít jasně definovanou bezpečnostní politiku. Velký význam mají také dobře proškolení a náležitě ohodnocení zaměstnanci, neboť lidé bývají nejslabším článkem v bezpečnostním řetězci.

V práci jsem také specifikoval jednotlivé síťové prvky, které se běžně vyskytují v IP sítích z pohledu bezpečného připojování. Zmíněné síťové prvky jsou základním kamenem pro konfiguraci bezpečného připojování. Uvedl a popsal jsem základní bezpečnostní protokoly pro bezpečné připojovaní. Při porovnání těchto protokolů musím konstatovat, že pro bezpečné propojení dvou nebo více LAN sítí se jako nejlepší jeví protokol IPSec, ale pro vzdálené připojování do sítě je mnohem efektivnější protokol SSL VPN, který umožňuje nastavit připojení do sítě přesně podle potřeb uživatele. SSL VPN se ještě bude velmi dynamicky rozvíjet a stane se hlavním způsobem bezpečného vzdáleného připojení pro uživatele.

V kontextu bezpečného připojování jsem se zmínil také o heslech, která jsou nedílnou součástí pro bezpečné přihlášení. Po porovnání všech druhů autentizace uživatele se jako nejvýhodnější jeví využití přihlašovacích systémů typu RSA token, oproti klasickému přihlašování se jménem a heslem. Při použití RSA tokenu je nutné zapamatovat si poměrně krátký PIN a přitom je připojování velmi bezpečné. Biometrické přihlašovací metody nejsou v současné době na takové úrovni, aby mohly nahradit stávající způsob přihlašování pomocí hesla nebo tokenů a čeká je ještě dlouhý vývoj.

V rámci praktické časti práce jsem se velmi podrobně seznámil se zařízením Juniper SA 6500 pro vzdálené přihlašování do sítě. Po detailním otestování možností Juniperu bych

rád konstatoval, že opravdu patří v tomto odvětví mezi špičku. Konfigurace Juniperu je velmi přehledná, jak jsem se snažil v práci dokumentovat. Při zavádění Juniperu do provozu je časově nejvíce náročnou fází navržení bezpečnostních pravidel pro jednotlivá oddělení firmy. Nastavení pravidel na zařízení již bylo poměrně jednoduché. Velkou nevýhodu u Juniper SA vidím v jeho licenční politice. Licenční politika je nastavena pro velké korporace a pro menši firmy je příliš nákladná. V závěru jsem také popsal problémy, které se po zavedení do provozu objevily. Hlavním problémem byl zvýšený provoz, který zapříčinil přetížení firewallu a problematická spolupráce webového mailového klienta s Juniper SA.

6 Použitá literatura

[1] Unix, [encyklopedie online], modifikováno 2010-02-10, dostupné z URL <http://en.wikipedia.org/wiki/Unix>, citováno 2010-02-15.

[2] BROWN, Arlene. VPNs: Only part of the remote access security solution. *Network Security*. vol. 2001, Issue 1. 2001. s. 12-14, ISSN 1353-4858.

[3] JIROVSKÝ, Václav. *Kybernetická kriminalita*. Grada Publishing a.s., 2007. 288 s. ISBN 978-80-247-1561-2.

[4] AMSEL, Ellen. Network security and access controls. *Computers & Security*. vol. 7, Issue 1. 1988. s. 53-57, ISSN 0167-4048.

[5] Fermat's Last Theorem, [encyklopedie online], modifikováno 2010-02-24, dostupné z URL <http://en.wikipedia.org/wiki/Fermat's_Last_Theorem>, citováno 2010-03-03.

[6] ZDRÁLEK, Jaroslav. Spolehlivost a diagnostika - Pasáž kódování, [studijní materiály online], publikováno 2007, dostupné z URL <http://kat454.vsb.cz/download/predmety/sad_071021_bst_01.pdf>, citováno 2009-10-15.

[7] Cisco Networking Academy: CCNA Exploration 4.0 – Network Fundamentals, 2007, [online příručka], dostupné z <http://cisco.netacad.net/>, citováno 2009-10-15.

[8] NORTHCUTT, Stephen a kol. *Bezpečnost počítačových sítí*. CP Books a.s. 2005. 589 s. ISBN 80-251-0697-7.

[9] KARGER, A. Paul. Authentication and discretionary access control in computer network. *Computers & Security*. vol. 5, Issue 4. 1986. s. 314-324, ISSN 0167-4048.

[10] PANDYA, Pramod. Local Area Network Security, In: John R. Vacca, Editor(s), *Computer and Information Security Handbook*. Morgan Kaufmann Boston. 2009. s. 149-167. ISBN 978-0-12-374354-1.

[11] McDERMOTT, Paul. Security in IP Networks. *Network Security*. vol. 2000, Issue 12. 2000. s. 7-9, ISSN 1353-4858.

[12] HARMENING, Jim, WRIGHT, Joe. Virtual Private Networks, In: John R. Vacca, Editor(s), *Computer and Information Security Handbook*. Morgan Kaufmann Boston. 2009. s. 507-517, ISBN 978-0-12-374354-1.

[13] IPSec, [encyklopedie online], modifikováno 2009-12-30, <http://cs.wikipedia.org/wiki/IPsec>, citováno 2010-03-27.

[14] HARDING, Andrew. SSL Virtual Private Networks. *Computers & Security*. vol. 22, Issue 5. 2003. s. 416-420, ISSN 0167-4048.

[15] *Configuring Juniper Networks Secure Access - Student Guide*, Revision 6.a, Juniper Networks Inc., 2007.

[16] KRATOŠ, J. *Implementace připojení do systému EduRoam*. Ostrava, 2007. 31 s. Bakalářská práce na Fakultě elektrotechniky a informatiky VŠB TUO na katedře telekomunikační techniky. Vedoucí práce Pavel Nevlud.

[17] WEEKS, Roger, DUMBILL, Edd, JEPSON, Brian. *A Complete Guide To Wireless Configuration Linux Unwired*. O'Reilly. 2004. 300 s. ISBN 0-596-00583-0.